COUNTING CLASSES OF SPECIAL POLYNOMIALS

Dissertation
zur
Erlangung des Doktorgrades (Dr. rer. nat.)
der
Mathematisch-Naturwissenschaftlichen Fakultät
der
Rheinischen Friedrich-Willhelms-Universität Bonn

vorgelegt von
Konstantin Ziegler
aus
München

Bonn, Juni 2014

Angefertigt mit Genehmigung der
Mathematisch-Naturwissenschaftlichen Fakultät der
Rheinischen Friedrich-Willhelms-Universität Bonn

1. Gutachter: Prof. Dr. Joachim von zur Gathen
2. Gutachter: Prof. Dr. Jens Franke
Tag der Promotion: 2. April 2015
Erscheinungsjahr: 2015

SYNOPSIS

Most integers are composite and most univariate polynomials over a finite field are reducible. The Prime Number Theorem and a classical result of Gauß count the remaining ones, approximately and exactly.

In two or more variables, the situation changes dramatically. Most multivariate polynomials are irreducible. We present counting results for some special classes of multivariate polynomials over a finite field, namely the *reducible* ones, the *s-powerful* ones (divisible by the s-th power of a nonconstant polynomial), and the *relatively irreducible* ones (irreducible but reducible over an extension field). These numbers come as exact formulas and as approximations with relative errors that essentially decrease exponentially in the input size.

Furthermore, a univariate polynomial f over a field F is *decomposable* if $f = g \circ h$ with nonlinear polynomials g and h. It is intuitively clear that the decomposable polynomials form a small minority among all polynomials. The *tame case*, where the characteristic p of F does not divide $n = \deg f$, is fairly well understood, and the upper and lower bounds on the number of decomposable polynomials of degree n match asymptotically. In the *wild case*, where p does divide n, the bounds are less satisfactory, in particular when p is the smallest prime divisor of n and divides n exactly twice.

There is an obvious inclusion-exclusion formula for counting. The main issue is then to determine, under a suitable normalization, the number of *collisions*, where essentially different components (g, h) yield the same f. In the tame case, Ritt's Second Theorem classifies all collisions of two such pairs. We provide a normal form for collisions of any number of compositions with any number of components. This generalization yields an exact formula for the number of decomposable polynomials of degree n coprime to p. For the wild case, we classify all collisions at degree $n = p^2$ and obtain the exact number of decomposable polynomials of degree p^2.

Keywords. univariate polynomials, multivariate polynomials, finite fields, counting special polynomials, enumerative combinatorics on polynomials, analytic combinatorics, generating functions, computer algebra, tame polynomial decomposition, wild polynomial decomposition, Ritt's Second Theorem

2010 Mathematics Subject Classification. 05A15 (Exact enumeration problems, generating functions), 11T06 (Polynomials), 12Y05 (Computational aspects of field theory and polynomials)

ZUSAMMENFASSUNG

Die meisten natürlichen Zahlen sind zusammengesetzt und die meisten univariaten Polynome über einem endlichen Körper sind reduzibel. Der Primzahlsatz und ein klassischer Satz von Gauß zählen näherungsweise und exakt die verbleibenden Elemente.

Bei Polynomen in zwei oder mehr Variablen wandelt sich das Bild. Die meisten multivariaten Polynome sind irreduzibel. Wir zeigen Zählergebnisse für Klassen multivariater Polynome über einem endlichen Körper, nämlich die *reduziblen*, die *s-potenzvollen* (teilbar duch die s-te Potenz eines nichtkonstanten Polynoms) und die *relativ irreduziblen* (irreduzibel, aber reduzibel in einer Körpererweiterung). Hierzu präsentieren wir exakte Formeln und Näherungen mit einem relativen Fehler der im Wesentlichen exponentiell in der Eingabegröße abnimmt.

Desweiteren ist ein univariates Polynom f über einem Körper F *zerlegbar*, wenn $f = g \circ h$ mit nichtlinearen Polynomen g und h. Es liegt intuitiv nahe, dass die zerlegbaren nur eine kleine Minderheit unter allen Polynomen darstellen. Der *zahme* Fall, wenn die Charakteristik p von F kein Teiler von $n = \deg f$ ist, ist gut erschlossen und untere und obere Schranke an die Zahl der zerlegbaren Polynome sind asymptotisch gleich. Im *wilden* Fall, wenn p ein Teiler von n ist, sind die Schranken gröber, insbesondere wenn p der kleinste Primteiler von n ist und n genau zweimal teilt.

Das Zählen mittels Inklusion-Exklusion liegt nahe, erfordert aber das Bestimmen von *Kollisionen*, dass heißt, unter geeigneter Normierung, verschiedener Komponenten (g, h) die das gleiche f ergeben. Im zahmen Fall klassifiziert der Zweite Satz von Ritt alle Kollisionen zweier solcher Paare. Wir zeigen eine Normalform für Kollisionen beliebig vieler Zusammensetzungen mit beliebig vielen Komponenten. Diese Verallgemeinerung liefert eine exakte Formel für die Anzahl der zerlegbaren Polynome vom Grad n, wenn n teilerfremd zu p ist. Im wilden Fall klassifizieren wir alle Kollisionen vom Grad $n = p^2$ und erhalten die genaue Anzahl der zerlegbaren Polynome vom Grad p^2.

CONTENTS

1

INTRODUCTION

I keep six honest serving-men
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who.[1]
— Rudyard Kipling

Why is it so hard to count[?][2]
— Doron Zeilberger

This introduction answers Kipling's questions. The remaining chapters address Zeilberger's.

1.1 WHY DO WE COUNT?

Die ganzen Zahlen hat der liebe Gott gemacht,
alles andere ist Menschenwerk.[3]
— Leopold Kronecker

Counting is good for everybody. It brings happiness,[4] helps democracy,[5] and starts sonnets.[6] It is also said to be a natural sleeping aid and tranquilizer. So it is no surprise that humans started counting at least 50 000 years ago (Eves, 1990, p. 9). Much more recently, the German ministry of education named 2008 *national year of mathematics* and chose "Mathematik – Alles, was zählt" [Mathematics – all that counts] as its slogan. In the same year, this author attended the crypt@b-it summer school at the University of Bonn and discussed his first counting task with his advisor-to-be on a hike to Castle Drachenfels. Six years later, this thesis is the outcome.

[1] The sources for the quotations are given on pages 137–138.
[2] [Text in brackets added by the author, also in other quotations.]
[3] God created the integers, all else is the work of man.
[4] See Venetia Evripiotou, *Counting Happiness*, short film, 2013.
[5] It's not the voting that's democracy, it's the counting. — Tom Stoppard
[6] How do I love thee? Let me count the ways. — Elizabeth Barrett Browning

For mathematicians, the benefits of counting mentioned above are pleasant extras, but as Hamming (1987, Preface) emphasizes, "[t]he purpose of computing is insight, not numbers." It is difficult to measure insight, but when queried for the most beautiful theorems, the readers of the Mathematical Intelligencer ranked six counting results among their top ten (Wells, 1990). Hence we ask, paraphrasing Wigner (1960), where this "surprising popularity of counting in mathematics" comes from?

A possible answer is given by the numerous proofs of existence based on counting and the pigeonhole principle. In this context, counting modulo two may provide a valuable shortcut. But existence is only half of the story. Lipton (2014) points out that "a common situation in complexity theory [is] where finding one object is easy, but finding the total number is hard." Examples include perfect matchings and satisfying assignments for formulas. This leads to another possible answer: counting results may be obtained via a clever parametrization. Here, explicit constructions and understanding of the (non)uniqueness of the parameters are means for counting but also of interest on their own. In this spirit, counting is simultaneously motivation, benchmark, and our ultimate test of understanding.

A classical counting task concerns the number $\pi(x)$ of primes less or equal than x. Results come in two flavors. On the one hand, the Prime Number Theorem says that asymptotically, a randomly chosen integer up to x is prime with probability *approximately* $1/\ln x$. The error term is then closely related to the zeros of the Riemann zeta-function. On the other hand, computing $\pi(x)$ *exactly* for ever increasing x is a traditional area of analytic number theory. The current world record is held by Franke, Kleinjung, Büthe & Jost (2014) with $\pi(10^{25}) = 176\,846\,309\,399\,143\,769\,411\,680$.

1.2 HOW IS THIS THESIS STRUCTURED AND WHAT DO WE COUNT?

> We can face our problem. We can arrange such facts as we have with order and method.
> — Hercule Poirot

In this thesis, we count classes of special polynomials over finite fields, approximately and exactly.

- In Part i (Chapter 2), we are interested in *multivariate* polynomials with special *factorization* patterns.
- In Part ii (Chapters 3–4), we investigate *univariate* polynomials with respect to their *decomposition* behavior.

We now highlight the main results. For more on the history and related work, we refer to the introduction of each part.

The analogue of the Prime Number Theorem for univariate polynomials over finite fields is a classical result of Gauß. A randomly chosen polynomial of degree n is irreducible with probability about $1/n$ and most univariate polynomials are composite. In two or more variables, the situation changes dramatically. Most multivariate polynomials are irreducible and Carlitz (1963) provides the first count of irreducible multivariate polynomials.

In Chapter 2, we provide exact formulas for the numbers of *reducible* (Sections 2.2–2.3), *s-powerful* (divisible by the sth power of a nonconstant polynomial, Section 2.4), and *relatively irreducible* polynomials (irreducible but reducible over an extension field, Section 2.5). The latter also yields the number of absolutely reducible polynomials. The formulas then lead to simple, yet precise, approximations to these numbers, with rapidly decaying relative errors. Our contributions are as follows.

- We provide exact formulas for the numbers under consideration using analytic combinatorics. These lead to easily implementable algorithms. The formulas are, however, not very transparent. Even the leading term is not immediately visible. (Theorems 2.2.7, 2.4.4, and 2.5.13).

- We use coefficient comparison to derive easy-to-use approximations to our numbers. The relative error is exponentially decreasing in the bit size of the data. However, it is given in big-Oh form and thus contains an unspecified constant (Theorems 2.2.16, 2.4.9, and 2.5.27).

- Finally, we present "second order" approximations to our numbers with explicit constants in the error term using a combinatorial counting method (Theorems 2.3.3, 2.4.20, and 2.5.32).

After this investigation of multivariate polynomials, we turn in Part ii to the decomposition of univariate polynomials.

The *composition* of two univariate polynomials $g, h \in F[x]$ over a field F is denoted as $f = g \circ h = g(h)$, and then (g, h) is a *decomposition* of f, and f is *decomposable* if g and h have degree at least 2. A fundamental dichotomy is between the *tame case*, where the characteristic p of F does not divide $\deg g$, and the *wild case*, where p divides $\deg g$. In the wild case, considerably less is known, both mathematically and computationally.

It is intuitively clear that the univariate decomposable polynomials form only a small minority among all univariate polynomials over a field. There is an obvious inclusion-exclusion formula for counting and the crux of the matter is to determine, under a suitable normalization, the number of *collisions*, where essentially different components (g, h) yield the same f. The number of decomposable polynomials of

degree n is thus the number of all pairs (g, h) with $\deg g \cdot \deg h = n$ reduced by the ambiguities introduced by collisions.

The task of counting compositions over a finite field of characteristic p was first considered by Giesbrecht (1988). He shows that the decomposable polynomials form an exponentially small fraction of all univariate polynomials. Von zur Gathen (2014a) presents general approximations for the number of decomposable polynomials of degree n. These come with satisfactory (rapidly decreasing) relative error bounds except when p divides n exactly twice. He also obtains explicit formulas for the number of decomposable polynomials of degree n when n has at most four divisors. We complement these results. In Chapter 3, we show how to quickly obtain explicit formulas at any degree coprime to p and in Chapter 4, we present approximations with satisfactory relative error bounds at degree p^2.

Two theorems by Ritt are the starting point for the study of collisions. Ritt's First Theorem relates all *complete* decompositions of a given polynomial, where all components are indecomposable. In this situation, Zieve & Müller (2008) study sequences of *Ritt moves*, where adjacent indecomposable g, h in a complete decomposition are replaced by g^*, h^* with the same composition, but $\deg g = \deg h^* \neq \deg h = \deg g^*$. Such collisions are the theme of Ritt's Second Theorem and von zur Gathen (2014b) presents a normal form with an exact description of the (non)uniqueness of the parameters.

In Chapter 3, we combine the above "normalizations" of Ritt's theorems to classify collisions of two or more decompositions, not necessarily complete and of arbitrary length. Our contributions are as follows.

- We obtain a normal form for collisions of compositions given by a set of degree sequences and determine exactly the (non)uniqueness of the parameters (Theorems 3.4.2 and 3.4.5).

- We derive an exact formula for the number of collisions at degree n over a finite field with characteristic coprime to n (Theorem 3.4.9).

- We conclude with a fast algorithm for the number of decomposable polynomials of degree n over a finite field of characteristic coprime to n (Algorithm 3.4.10).

In Chapter 4, we turn to the wild case. The previously known approximations come with satisfactory (rapidly decreasing) relative error bounds except when p divides $n = \deg f$ exactly twice. The main result of this chapter (Theorem 4.5.6) determines exactly the number of decomposable polynomials in one of these difficult cases, namely when $n = p^2$ and hence $\deg g = \deg h = p$. Our contributions are as follows.

- We provide explicit constructions for collisions at degree r^2, where r is a power of the characteristic $p > 0$ (Fact 4.2.1, Theorem 4.2.22).
- We provide a classification of all collisions at degree p^2, linking every collision to a unique explicit construction (Theorem 4.4.9).
- We use these two results to obtain an exact formula for the number of decomposable polynomials at degree p^2 (Theorem 4.5.6).
- The classification yields an efficient algorithm to test whether a given polynomial of degree p^2 has a collision or not (Algorithm 4.4.14).

1.3 WHO, WHERE, AND WHEN?

> What we know is a drop,
> what we don't know, an ocean.
> — Isaac Newton

Many people have contributed in various ways to the research in this thesis. You meet them implicitly throughout this thesis and explicitly in the acknowledgements at the end. Here, we merely summarize the publication history of each chapter.

The results of Chapter 2 are joint work with Joachim von zur Gathen and Tuba Viola. We presented them at the meeting of the German Fachgruppe Computeralgebra 2009 in Kassel, Germany, and at LATIN 2010 in Oaxaca, Mexico. They have been published as

- Joachim von zur Gathen, Alfredo Viola & Konstantin Ziegler (2013). Counting reducible, powerful, and relatively irreducible multivariate polynomials over finite fields. *SIAM Journal on Discrete Mathematics* **27**(2), 855–891. URL `http://dx.doi.org/10.1137/110854680`. Also available at `http://arxiv.org/abs/0912.3312`. Extended abstract in *Proceedings of LATIN 2010, Oaxaca, Mexico* (2010).

The results of Chapter 3 have been presented at the meeting of the German Fachgruppe Computeralgebra 2014 in Kassel, Germany, at the CRM Workshop on Polynomials over Finite Fields 2014 in Barcelona, Spain, and at ISSAC 2014 in Kobe, Japan. They are available as

- Konstantin Ziegler (2014). Tame decompositions and collisions. *Submitted*, 35 pages. URL `http://arxiv.org/abs/1402.5945`. Extended abstract in *Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation ISSAC '14, Kobe, Japan* (2014), 421–428.

The results of Chapter 4 are joint work with Raoul Blankertz and Joachim von zur Gathen. We presented them at the meeting of the German Fachgruppe Computeralgebra 2012 in Kassel, Germany, at ISSAC 2012 in Grenoble, France, at the BIRS Workshop on The Art of Iterating Rational Functions over Finite Fields 2013 in Banff, Canada, and at the Symbolic Computation Seminar, 2013, in Waterloo, Canada. They have been published as

- Raoul Blankertz, Joachim von zur Gathen & Konstantin Ziegler (2013). Compositions and collisions at degree p^2. *Journal of Symbolic Computation* **59**, 113–145. ISSN 0747-7171. URL `http://dx.doi.org/10.1016/j.jsc.2013.06.001`. Also available at `http://arxiv.org/abs/1202.5810`. Extended abstract in *Proceedings of the 2012 International Symposium on Symbolic and Algebraic Computation ISSAC '12, Grenoble, France* (2012), 91–98.

Concise versions of some results also appeared in the survey of von zur Gathen & Ziegler (2015).

Part I

MULTIVARIATE POLYNOMIALS

I have often wished, that I had employed about the speculative part of geometry, and the cultivation of the specious Algebra [multivariate polynomials] I had been taught very young, a good part of that time and industry, that I had spent about surveying and fortification (of which I remember I once wrote an entire treatise) and other practick parts of mathematicks. And indeed the operations of symbolical arithmetick (or the modern Algebra) seem to me to afford men one of the clearest exercises of reason that I ever yet met with.

— Robert Boyle

2

COUNTING MULTIVARIATE POLYNOMIALS

The More Variables, the Better?
— Dick Lipton

An earlier version of this chapter appeared as von zur Gathen, Viola & Ziegler (2013), see Section 1.3 for the complete publication history.

Concerning special classes of univariate polynomials over a finite field, Zsigmondy (1894) counts those with a given number of distinct roots or without irreducible factors of a given degree. In the same situation, Artin (1924) counts the irreducible ones in an arithmetic progression and Hayes (1965) generalizes these results. Cohen (1969) and Car (1987) count polynomials with certain factorization patterns and Williams (1969) those with irreducible factors of given degree. Polynomials that occur as a norm in field extensions are studied by Gogia & Luthar (1981).

In two or more variables, the situation changes dramatically. Most multivariate polynomials are irreducible. Carlitz (1963) provides the first count of irreducible multivariate polynomials. In Carlitz (1965), he goes on to study the fraction of irreducibles when bounds on the degrees in each variable are prescribed; see also Cohen (1968). In this work, we opt for bounding the total degree because it has the charm of being invariant under invertible linear transformations. Gao & Lauder (2002) consider the counting problem in yet another model, namely where one variable occurs with maximal degree. The natural generating function (or zeta function) for the irreducible polynomials in two or more variables does not converge anywhere outside of the origin. Wan (1992) notes that this explains the lack of a simple combinatorial formula for the number of irreducible polynomials. But he gives a p-adic formula, and also a (somewhat complicated) combinatorial formula. For further references, see Mullen & Panario (2013, Section 3.6).

In the bivariate case, von zur Gathen (2008) proves precise approximations with an exponentially decreasing relative error. Bodin (2008) gives a recursive formula for the number of irreducible bivariate polynomials and remarks on a generalization for more than two variables;

he follows up with Bodin (2010). Further types of multivariate polynomials are examined from a counting perspective: decomposable ones (Bodin, Dèbes & Najib, 2009, von zur Gathen, 2011), singular ones (von zur Gathen, 2008), and pairs of coprime polynomials (Hou & Mullen, 2009).

This chapter provides exact formulas for the numbers of reducible (Sections 2.2–2.3), s-powerful (Section 2.4), and relatively irreducible polynomials (Section 2.5). The latter also yields the number of absolutely reducible polynomials. Of these, only reducible polynomials have been treated in the literature, usually with much larger error terms. The formulas also yield simple, yet precise, approximations to these numbers, with rapidly decaying relative errors.

We use two different methodologies to obtain such bounds: generating functions and combinatorial counting. The usual approach, see Flajolet & Sedgewick (2009), of analytic combinatorics on series with integer coefficients leads, in our case, to power series that diverge everywhere (except at 0). We have not found a way to make this work. Instead, we use power series with symbolic coefficients, namely rational functions in a variable representing the field size. Several useful relations from standard analytic combinatorics carry over to this new scenario. In a first step, this yields in a straightforward manner exact formulas for the numbers under consideration (Theorems 2.2.7, 2.4.4, and 2.5.13). These formulas are, however, not very transparent. Even the leading term is not immediately visible.

In a second step, coefficient comparisons yield easy-to-use approximations to our numbers (Theorems 2.2.16, 2.4.9, and 2.5.27). The relative error is exponentially decreasing in the bit size of the data. As an example, Theorem 2.2.16 gives a "third order" approximation for the number of reducible polynomials, and thus a "fourth order" approximation for the irreducible ones. The error term is in big-Oh form and thus contains an unspecified constant.

In a third step, a different method, namely some combinatorial counting, yields "second order" approximations with explicit constants in the error term (Theorems 2.3.3, 2.4.20, and 2.5.32).

Geometrically, a single polynomial corresponds to a hypersurface, that is, to a cycle in affine or projective space, of codimension 1. This correspondence preserves the respective notions of reducibility. Thus, Sections 2.2–2.3 can also be viewed as counting reducible hypersurfaces, in particular, planar curves, and Section 2.4 those with an s-fold component. Reducible curves embedded in higher-dimensional spaces, parametrized by the appropriate Chow variety, are counted by Cesaratto, von zur Gathen & Matera (2013).

We conclude with open questions and suggestions for future work in Section 2.6.

2.1 NOTATION

> The method used in proving these and similar results is not elementary in that it depends on equating coefficients in equal power series. However it appears to be the natural one for the subject, and there seems to be little point to recasting the proofs in "arithmetic" shape.
>
> — Leonard Carlitz

We work in the polynomial ring $F[x_1, \dots, x_r]$ in $r \geqslant 1$ variables over a field F and consider polynomials with total degree equal to some nonnegative integer n:

$$P^{\mathrm{all}}_{r,n}(F) = \{f \in F[x_1, \dots, x_r] \colon \deg f = n\}.$$

The polynomials of degree at most n form an F-vector space of dimension

$$b_{r,n} = \binom{r+n}{r} = \frac{(r+n)^{\underline{r}}}{r!},$$

where the *falling factorial* or *Pochhammer symbol* is

$$(r+x)^{\underline{r}} = (r+x) \cdot (r-1+x) \cdots (1+x), \tag{2.1.1}$$

for any real x and any nonnegative integer r, see Knuth (1992). Over a finite field $\mathbb{F}_q$ with q elements, we have

$$\#P^{\mathrm{all}}_{r,n}(\mathbb{F}_q) = q^{b_{r,n}} - q^{b_{r,n-1}} = q^{b_{r,n}}(1 - q^{-b_{r-1,n}}).$$

The property of a certain polynomial to be reducible, squareful or relatively irreducible is shared with all polynomials associated to the given one. For counting them, it is sufficient to take one representative. We choose an arbitrary monomial order, say, the degree-lexicographic one, so that the monic polynomials are those with leading coefficient 1, and write

$$P_{r,n}(F) = \{f \in P^{\mathrm{all}}_{r,n}(F) \colon f \text{ is monic}\}.$$

Then

$$\#P_{r,n}(\mathbb{F}_q) = \frac{\#P^{\mathrm{all}}_{r,n}(\mathbb{F}_q)}{q-1} = q^{b_{r,n}-1}\frac{1 - q^{-b_{r-1,n}}}{1 - q^{-1}}. \tag{2.1.2}$$

The product of two monic polynomials is again monic.

Our exact formulas are derived using a generating series, the standard tool in analytic combinatorics as presented in Flajolet & Sedgewick (2009) by two experts who created large parts of the theory. We first recall a few general primitives from this theory that enable one to set up symbolic equations for generating functions starting from combinatorial specifications. A countable set $\mathcal{C}$ with a "size"

function $|\cdot|\colon \mathcal{C} \to \mathbb{Z}_{\geqslant 0}$ is called a *combinatorial class* if the preimage of any $n \in \mathbb{Z}_{\geqslant 0}$ is finite. The number of elements of size n is denoted by C_n and these numbers are encoded in the *generating function* $C(z)$ of the sequence C_n:

$$C(z) = \sum_{n \geqslant 0} C_n z^n \in \mathbb{Z}_{\geqslant 0}[\![z]\!].$$

We sometimes omit the argument z. Before we tackle the task of counting polynomials, let us recall some basics about power series. An element in the ring of univariate power series over a ring is invertible if and only if its constant term is invertible. We call a power series *original* if its constant term vanishes, so that its graph passes through the origin. The power series

$$\log(1-z) = -\sum_{n \geqslant 1} \frac{z^n}{n} \in \mathbb{Q}[\![z]\!] \tag{2.1.3}$$

is original and substituting a power series f in another power series g is well-defined if f is original.

Two combinatorial classes $\mathcal{A}$ and $\mathcal{B}$ are *isomorphic* if there is a size-preserving bijection $\mathcal{A} \to \mathcal{B}$ or equivalently if the generating functions A and B, respectively, are equal. We recall three basic constructions of new combinatorial classes from given ones; see Flajolet & Sedgewick (2009, Section I. 2.).

Let $\mathcal{A}$ and $\mathcal{B}$ be two combinatorial classes. We define the *disjoint union*

$$\mathcal{A} \dot\cup \mathcal{B} = \{\{0\} \times \mathcal{A}\} \cup \{\{1\} \times \mathcal{B}\}.$$

The size of an element $(0, a)$ or $(1, b)$ is defined as the size of a or b, respectively. We also define the *sequence class*

$$\mathcal{SEQ}(\mathcal{A}) = \{(\alpha_1, \ldots, \alpha_\ell)\colon \ell \geqslant 0, \alpha_i \in \mathcal{A}\},$$

where $|(\alpha_1, \ldots, \alpha_\ell)| = \sum_i |\alpha_i|$. This is a combinatorial class, if $\mathcal{A}$ contains no element of size 0. Finally, we derive the *multiset class*

$$\mathcal{MSET}(\mathcal{A}) = \mathcal{SEQ}(\mathcal{A})/\sim,$$

where $(\alpha_1, \ldots, \alpha_\ell) \sim (\beta_1, \ldots, \beta_\ell)$ if there is a permutation σ of $\{1, \ldots, \ell\}$ such that $\alpha_i = \beta_{\sigma(i)}$ for all i. This class contains all finite sequences of elements from $\mathcal{A}$ where repetition is allowed, but ordering is ignored. The generating functions for these constructions are classic applications of combinatorics.

Fact 2.1.4 (see Flajolet & Sedgewick, 2009, Theorems I.1 and I.5)**.** *Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be combinatorial classes with generating functions* A, B, *and* C, *respectively.*

(i) If $\mathcal{A} = \mathcal{B} \dot\cup \mathcal{C}$, *then* $A = B + C$.

(ii) If $\mathcal{A} = \mathcal{MSET}(\mathcal{B})$ *and* $B_0 = 0$, *then*

$$B = \sum_{k \geqslant 1} \frac{\mu(k)}{k} \log(A(z^k)),$$

where μ *is the number-theoretic Möbius-function, defined as*

$$\mu(k) = \begin{cases} 1 & \text{if } k = 1, \\ (-1)^\ell & \text{if } k \text{ is the product of } \ell \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

2.2 GENERATING FUNCTIONS FOR REDUCIBLE POLYNOMIALS

> Practice yourself, for heaven's sake, in little things;
> and thence proceed to greater.
> — Epictetus

> "Excellent!", I cried. "Elementary", he said.
> — John H. Watson

To study reducible polynomials, we consider the following subsets of $P_{r,n}(F)$:

$$\begin{aligned} I_{r,n}(F) &= \{f \in P_{r,n}(F) \colon f \text{ is irreducible}\}, \\ R_{r,n}(F) &= P_{r,n}(F) \setminus I_{r,n}(F). \end{aligned}$$

In the usual notions, the polynomial 1 is neither reducible nor irreducible. In our context, it is natural to have $R_{r,0}(F) = \{1\}$ and $I_{r,0}(F) = \varnothing$.

The sets of polynomials

$$\begin{aligned} \mathcal{P} &= \bigcup_{n \geqslant 0} P_{r,n}(\mathbb{F}_q), \\ \mathcal{I} &= \bigcup_{n \geqslant 0} I_{r,n}(\mathbb{F}_q), \\ \mathcal{R} &= \mathcal{P} \setminus \mathcal{I}, \end{aligned}$$

are combinatorial classes with the total degree as size functions and we denote the corresponding generating functions by $P, I, R \in \mathbb{Z}_{\geqslant 0}[\![z]\!]$, respectively. Their coefficients are

$$P_n = P_{r,n}(\mathbb{F}_q) = \#P_{r,n}(\mathbb{F}_q) = q^{b_{r,n}-1} \frac{1 - q^{-b_{r-1,n}}}{1 - q^{-1}}, \qquad (2.2.1)$$

$$\begin{aligned} R_n &= R_{r,n}(\mathbb{F}_q) = \#R_{r,n}(\mathbb{F}_q), \\ I_n &= I_{r,n}(\mathbb{F}_q) = \#I_{r,n}(\mathbb{F}_q), \end{aligned}$$

```
allpolysGF:=proc(z,N,r) local i: option remember:
    sum('simplify((q^binomial(r+i,r)-q^binomial(r+i-1,r))/
        (q-1))*z^i',i=0..N):
end:

irreduciblesGF:=proc(z,N,r) local k: option remember:
    convert(taylor((sum('mobius(k)/k*
        log(allpolysGF(z^k,N,r))',k=1..N)),z,N+1),
            polynom):
end:

reduciblesGF:=proc(z,N,r) option remember:
    allpolysGF(z,N,r)-irreduciblesGF(z,N,r):
end:

reducibles:=proc(n,r)
coeff(sort(expand(reduciblesGF(z,n,r))),z^n):
end:
```

Figure 2.2.4: Maple program to compute the number of monic reducible polynomials in r variables of degree n.

respectively, dropping $\mathbb{F}_q$ and r from the notation. By definition, $\mathcal{P}$ is isomorphic to the disjoint union of $\mathcal{R}$ and $\mathcal{I}$, and therefore

$$R = P - I \tag{2.2.2}$$

by Fact 2.1.4 (i). By unique factorization, every element in $\mathcal{P}$ corresponds to an unordered finite sequence of irreducible polynomials, where repetition is allowed. Hence $\mathcal{P}$ is isomorphic to $\mathcal{MSET}(\mathcal{I})$ and by Fact 2.1.4 (ii),

$$I = \sum_{k \geqslant 1} \frac{\mu(k)}{k} \log P(z^k). \tag{2.2.3}$$

A Maple implementation of the resulting algorithm to compute the number of reducible polynomials is described in Figure 2.2.4. It is easy to program and execute and was used to calculate the number of bivariate reducible polynomials in von zur Gathen (2008, Table 2.1). We extend these exact results in Table 2.2.5.

This approach quickly leads to explicit formulas. For a positive integer n, a *composition* of n is a sequence $j = (j_1, j_2, \ldots, j_{|j|})$ of positive integers $j_1, j_2, \ldots, j_{|j|}$ with $j_1 + j_2 + \cdots + j_{|j|} = n$, where $|j|$ denotes the length of the sequence. We define the set

$$M_n = \{\text{compositions of } n\}. \tag{2.2.6}$$

n	$\#R_{3,n}(\mathbb{F}_q)$
1	0
2	$(q^6+2q^5+3q^4+3q^3+2q^2+q)/2$
3	$(3q^{12}+6q^{11}+9q^{10}+8q^9+6q^8+3q^7-q^6-3q^5-3q^4+q^2+q)/3$
4	$(4q^{22}+8q^{21}+12q^{20}+12q^{19}+14q^{18}+16q^{17}+18q^{16}+16q^{15}+10q^{14}-13q^{12}-20q^{11}-20q^{10}-10q^9-q^8+6q^7+7q^6+4q^5-2q^3-q^2)/4$
5	$(5q^{37}+10q^{36}+15q^{35}+15q^{34}+15q^{33}+15q^{32}+15q^{31}+15q^{30}+15q^{29}+20q^{28}+25q^{27}+30q^{26}+30q^{25}+25q^{24}+15q^{23}-15q^{21}-30q^{20}-45q^{19}-60q^{18}-65q^{17}-55q^{16}-26q^{15}+10q^{14}+40q^{13}+50q^{12}+40q^{11}+19q^{10}-10q^8-10q^7-5q^6-q^5+q^3+q^2+q)/5$
6	$(6q^{58}+12q^{57}+18q^{56}+18q^{55}+18q^{54}+18q^{53}+18q^{52}+18q^{51}+18q^{50}+18q^{49}+18q^{48}+18q^{47}+18q^{46}+18q^{45}+18q^{44}+24q^{43}+30q^{42}+36q^{41}+36q^{40}+30q^{39}+21q^{38}+6q^{37}-3q^{36}-6q^{35}-3q^{34}+3q^{32}-6q^{31}-27q^{30}-60q^{29}-99q^{28}-128q^{27}-141q^{26}-132q^{25}-104q^{24}-60q^{23}-3q^{22}+70q^{21}+144q^{20}+201q^{19}+203q^{18}+147q^{17}+51q^{16}-45q^{15}-102q^{14}-105q^{13}-71q^{12}-27q^{11}+3q^{10}+14q^9+11q^8+5q^7+3q^6+3q^5+2q^4-2q^3-2q^2-q)/6$

n	$\#R_{4,n}(\mathbb{F}_q)$
1	0
2	$(q^8+2q^7+3q^6+4q^5+4q^4+3q^3+2q^2+q)/2$
3	$(3q^{18}+6q^{17}+9q^{16}+12q^{15}+12q^{14}+12q^{13}+11q^{12}+9q^{11}+6q^{10}+2q^9-3q^8-6q^7-7q^6-6q^5-2q^4+q^2+q)/3$
4	$(4q^{38}+8q^{37}+12q^{36}+16q^{35}+16q^{34}+16q^{33}+16q^{32}+16q^{31}+16q^{30}+16q^{29}+18q^{28}+20q^{27}+22q^{26}+24q^{25}+26q^{24}+28q^{23}+26q^{22}+20q^{21}+10q^{20}-4q^{19}-22q^{18}-36q^{17}-45q^{16}-48q^{15}-42q^{14}-34q^{13}-21q^{12}-6q^{11}+8q^{10}+18q^9+20q^8+16q^7+9q^6+2q^5-2q^4-2q^3-q^2)/4$

n	$\#R_{5,n}(\mathbb{F}_q)$
1	0
2	$(q^{10}+2q^9+3q^8+4q^7+5q^6+5q^5+4q^4+3q^3+2q^2+q)/2$
3	$(3q^{25}+6q^{24}+9q^{23}+12q^{22}+15q^{21}+15q^{20}+15q^{19}+15q^{18}+15q^{17}+15q^{16}+14q^{15}+12q^{14}+9q^{13}+5q^{12}-6q^{10}-10q^9-12q^8-12q^7-10q^6-5q^5-2q^4+q^2+q)/3$
4	$(4q^{60}+8q^{59}+12q^{58}+16q^{57}+20q^{56}+20q^{55}+20q^{54}+20q^{53}+20q^{52}+20q^{51}+20q^{50}+20q^{49}+20q^{48}+20q^{47}+20q^{46}+20q^{45}+20q^{44}+20q^{43}+20q^{42}+20q^{41}+22q^{40}+24q^{39}+26q^{38}+28q^{37}+30q^{36}+32q^{35}+34q^{34}+36q^{33}+38q^{32}+40q^{31}+38q^{30}+32q^{29}+22q^{28}+8q^{27}-10q^{26}-32q^{25}-50q^{24}-64q^{23}-74q^{22}-80q^{21}-79q^{20}-78q^{19}-74q^{18}-66q^{17}-53q^{16}-34q^{15}-12q^{14}+10q^{13}+29q^{12}+42q^{11}+45q^{10}+40q^9+30q^8+18q^7+7q^6-2q^4-2q^3-q^2)/4$

Table 2.2.5: Exact values of $\#R_{r,n}(\mathbb{F}_q)$ for small values of r and n. For $n<4$, these are the numbers given in Theorem 2.2.16.

This standard combinatorial notion is not to be confused with the composition of polynomials in Part ii.

Theorem 2.2.7. *For* $r \geqslant 1$, $q \geqslant 2$, *and* P_n *as in* (2.2.1), *we have*

$$\begin{aligned} I_0 &= 0, \\ I_n &= -\sum_{k \mid n} \frac{\mu(k)}{k} \sum_{j \in M_{n/k}} \frac{(-1)^{|j|}}{|j|} P_{j_1} P_{j_2} \cdots P_{j_{|j|}}, \end{aligned}$$

for $n \geqslant 1$, *and therefore*

$$\begin{aligned} R_0 &= 1, \\ R_n &= P_n + \sum_{k \mid n} \frac{\mu(k)}{k} \sum_{j \in M_{n/k}} \frac{(-1)^{|j|}}{|j|} P_{j_1} P_{j_2} \cdots P_{j_{|j|}}, \end{aligned}$$

for $n \geqslant 1$.

Proof. We consider the original power series $F = 1 - P = -\sum_{i \geqslant 1} P_i z^i$. The Taylor expansion (2.1.3) of $\log(1 - F(z^k))$ in (2.2.3) yields

$$\begin{aligned} I &= -\sum_{k \geqslant 1} \frac{\mu(k)}{k} \sum_{i \geqslant 1} \frac{F(z^k)^i}{i} = -\sum_{k \geqslant 1} \frac{\mu(k)}{k} \sum_{i \geqslant 1} \frac{(-1)^i}{i} \Big(\sum_{j \geqslant 1} P_j z^{jk} \Big)^i \\ &= -\sum_{k \geqslant 1} \frac{\mu(k)}{k} \sum_{i \geqslant 1} \frac{(-1)^i}{i} (P_1 z^k + P_2 z^{2k} + P_3 z^{3k} + \dots)^i, \\ I_0 &= 0, \\ I_n &= -\sum_{k \mid n} \frac{\mu(k)}{k} \sum_{i \geqslant 1} \frac{(-1)^i}{i} \sum_{\substack{j \in M_{n/k} \\ |j| = i}} P_{j_1} P_{j_2} \cdots P_{j_i}, \end{aligned}$$

for $n \geqslant 1$, which proves the claimed formulas for I. The results for R follow by (2.2.2). □

We check that the formula yields the well-known one, see Lidl & Niederreiter (1997, Theorem 3.25), in the univariate case, where $r = 1$. We then have $P_j = q^j$ and so $P_{j_1} P_{j_2} \cdots P_{j_i} = q^{n/k}$ for any composition $j_1 + j_2 + \cdots + j_i = n/k$. Moreover, the number of compositions of m with i components is $\binom{m-1}{i-1}$, see Flajolet & Sedgewick (2009, Section I.3.1). As a consequence we have for k dividing n

$$\begin{aligned} \sum_{\substack{j \in M_{n/k} \\ |j| = i}} \frac{(-1)^i}{i} P_{j_1} P_{j_2} \cdots P_{j_i} &= q^{n/k} \sum_{i \geqslant 1} \frac{(-1)^i}{i} \binom{n/k - 1}{i - 1} \\ &= \frac{k q^{n/k}}{n} \sum_{i \geqslant 1} (-1)^i \binom{n/k}{i} = -\frac{k q^{n/k}}{n}, \\ I_n &= \frac{1}{n} \sum_{k \mid n} \mu(k) q^{n/k}. \end{aligned} \tag{2.2.8}$$

Cohen (1968) notes that, compared to the univariate case, "the situation is different and much more difficult. In this case, no explicit formula [...] is available."

For $r \geqslant 2$, the power series P, I, and R do not converge anywhere except at 0, and the standard asymptotic arguments of analytic combinatorics are inapplicable. We now deviate from this approach and move from power series in $\mathbb{Q}[\![z]\!]$ to power series in $\mathbb{Q}(\mathbf{q})[\![z]\!]$, where $\mathbf{q}$ is a symbolic variable representing the field size. For $r \geqslant 2$ and $n \geqslant 0$ we let

$$P_n(\mathbf{q}) = P_{r,n}(\mathbf{q}) = \mathbf{q}^{b_{r,n}-1}\frac{1-\mathbf{q}^{-b_{r-1,n}}}{1-\mathbf{q}^{-1}} \in \mathbb{Z}[\mathbf{q}], \tag{2.2.9}$$

where we usually omit r from the notation. As examples, we have

$$P_0(\mathbf{q}) = 1, P_1(\mathbf{q}) = \mathbf{q}^r\frac{1-\mathbf{q}^{-r}}{1-\mathbf{q}^{-1}}, \text{ and } P_2(\mathbf{q}) = \mathbf{q}^{r(r+3)/2}\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-1}}. \tag{2.2.10}$$

We define the power series $P, I, R \in \mathbb{Q}(\mathbf{q})[\![z]\!]$ by

$$P(\mathbf{q}, z) = \sum_{n\geqslant 0} P_n(\mathbf{q})z^n, \tag{2.2.11}$$

$$I(\mathbf{q}, z) = \sum_{k\geqslant 1} \frac{\mu(k)}{k}\log P(\mathbf{q}, z^k), \tag{2.2.12}$$

$$R(\mathbf{q}, z) = P(\mathbf{q}, z) - I(\mathbf{q}, z).$$

Now $1 - P(\mathbf{q}, z^k)$ is an original power series, and $\log P(\mathbf{q}, z^k)$ and I are well-defined, with $I(\mathbf{q}, 0) = 0$. For $q \in \mathbb{Q}$, the rational functions in $\mathbb{Q}(\mathbf{q})$ without pole at $\mathbf{q} \leftarrow q$ form a ring, the localization $\mathbb{Q}[\mathbf{q}]_{(\mathbf{q}-q)}$. If we restrict the power series coefficients to this ring, the evaluation map which substitutes an integer q for $\mathbf{q}$ is a ring homomorphism. Since P_n is actually a polynomial in $\mathbf{q}$, this poses no restriction in our case, and evaluating $\mathbf{q} \leftarrow q$ maps $P(\mathbf{q}, z)$ to $P(z)$ coefficientwise. In other words, the coefficient of z^n equals

$$[z^n]P(q, z) = P_n$$

by (2.1.2). Furthermore, I and R relate to P in the same way as I and R do to P, so that

$$[z^n]I(q, z) = I_n,$$
$$[z^n]R(q, z) = R_n.$$

The formula of Theorem 2.2.7 is exact but somewhat cumbersome. A main goal in this chapter is to find simple yet precise approximations, with rapidly decaying error terms. We fix some notation. For nonzero $f \in \mathbb{Q}(\mathbf{q})$, $\deg_{\mathbf{q}} f$ is the degree of f, that is, the numerator degree minus the denominator degree. Thus $\deg_{\mathbf{q}} P_n = b_{r,n} - 1$ and

$\deg_{\mathbf{q}}(f+g) \leqslant \max\{\deg_{\mathbf{q}} f, \deg_{\mathbf{q}} g\}$. The appearance of $O(\mathbf{q}^{-m})$ with a positive integer m in an equation means the existence of some f with degree at most $-m$ that makes the equation valid. The charm of our approach is that we obtain results for any "fixed" r and n. If a term $O(\mathbf{q}^{-m})$ appears, then we may conclude a numerical asymptotic result for growing prime powers q.

We start with a degree comparison for certain products of the $P_i(\mathbf{q})$ and sometimes omit the argument $\mathbf{q}$.

Lemma 2.2.13. *Let $r \geqslant 2$ and $n \geqslant 0$.*

(i) For $i, j \geqslant 0$, we have $\deg_{\mathbf{q}}(P_i \cdot P_j) \leqslant \deg_{\mathbf{q}} P_{i+j}$, with equality if and only if $ij = 0$.

(ii) For $1 \leqslant k \leqslant n/2$, the sequence of integers $\deg_{\mathbf{q}}(P_k \cdot P_{n-k})$ is strictly decreasing in k.

(iii) For $3 \leqslant k \leqslant n/2$, we have $\deg_{\mathbf{q}} P_1^2 P_{n-2} \geqslant \deg_{\mathbf{q}} P_k P_{n-k}$, with equality only for $(r, n, k) = (2, 6, 3)$.

Proof. (i) The claimed inequality is equivalent to

$$\binom{r+i}{r} + \binom{r+j}{r} - 1 \leqslant \binom{r+i+j}{r},$$

which follows by considering the choices of r-element subsets from a set with $r+i+j$ elements. Since $r \geqslant 2$, this inequality is strict if and only if both i and j are nonzero.

(ii) Using (2.2.9), we define a function u as

$$u(k) = \deg_{\mathbf{q}}(P_k \cdot P_{n-k}) = \binom{r+k}{r} + \binom{r+n-k}{r} - 2. \quad (2.2.14)$$

We extend the domain of $u(k)$ to real numbers k between 1 and $n/2$ by means of falling factorials as in (2.1.1)

$$u(k) = \frac{(r+k)^{\underline{r}}}{r!} + \frac{(r+n-k)^{\underline{r}}}{r!} - 2.$$

It is sufficient to show that the affine transformation $\bar{u}$ with

$$\bar{u}(k) = r! \cdot (u(k) + 2) = (r+k)^{\underline{r}} + (r+n-k)^{\underline{r}}$$

is strictly decreasing. The first derivative with respect to k is

$$\bar{u}'(k) = \sum_{1 \leqslant i \leqslant r} \Big(\frac{(r+k)^{\underline{r}}}{i+k} - \frac{(r+n-k)^{\underline{r}}}{i+n-k} \Big).$$

Since $0 < i+k < i+n-k$ for $1 < k < n/2$, each difference is negative, and so is $\bar{u}'(k)$.

(iii) Since $r \geqslant 2$ we have

$$\begin{aligned}(r-2)(r-1)(r+5) &\geqslant 0,\\ b_{r-1,4} &\geqslant b_{r,3} - 2r - 1,\\ 2r + b_{r,4} - 1 &\geqslant 2b_{r,3} - 2,\\ \deg_{\mathbf{q}} P_1^2 P_4 &\geqslant \deg_{\mathbf{q}} P_3 P_3,\end{aligned} \tag{2.2.15}$$

and equality if and only if $r = 2$. This proves the claimed inequality for $n = 6$.

For $n > 6$ we have $b_{r-1,n-2} > b_{r-1,4}$ and with (2.2.15) follows

$$\begin{aligned}b_{r-1,n-2} &> b_{r,3} - 2r - 1,\\ 2r + b_{r,n-2} - 1 &> b_{r,3} + b_{r,n-3} - 2,\\ \deg_{\mathbf{q}} P_1^2 P_{n-2} &> \deg_{\mathbf{q}} P_3 P_{n-3},\end{aligned}$$

which proves (iii) for $k = 3$ and by the monotonicity proven in (ii) also for all larger k. □

Theorem 2.2.16. *Let* $r \geqslant 2$ *and*

$$\rho_{r,n}(\mathbf{q}) = \mathbf{q}^{\binom{r+n-1}{r}+r-1}\frac{1-\mathbf{q}^{-r}}{(1-\mathbf{q}^{-1})^2} \in \mathbb{Q}(\mathbf{q}). \tag{2.2.17}$$

Then

$$\begin{aligned}R_0 &= 1,\\ R_1 &= 0,\\ R_2 &= \frac{\rho_{r,2}(\mathbf{q})}{2}\cdot(1-\mathbf{q}^{-r-1}),\\ R_3 &= \rho_{r,3}(\mathbf{q})\Big(1-\mathbf{q}^{-r(r+1)/2}+\mathbf{q}^{-r(r-1)/2}\frac{1-2\mathbf{q}^{-r}+2\mathbf{q}^{-2r-1}-\mathbf{q}^{-2r-2}}{3(1-\mathbf{q}^{-1})}\Big),\\ R_4 &= \rho_{r,4}(\mathbf{q})\cdot\Big(1+\mathbf{q}^{-\binom{r+1}{3}}\cdot\frac{1+O(\mathbf{q}^{-r(r-1)/2})}{2(1-\mathbf{q}^{-r})}\Big),\end{aligned} \tag{2.2.18}$$

and for $n \geqslant 5$

$$R_n = \rho_{r,n}(\mathbf{q})\cdot\Big(1+\mathbf{q}^{-\binom{r+n-2}{r-1}+r(r+1)/2}\cdot\frac{1+O(\mathbf{q}^{-r(r-1)/2})}{1-\mathbf{q}^{-r}}\Big). \tag{2.2.19}$$

Proof. We start the symbolic analog of our approach in the proof of Theorem 2.2.7 with the original power series $F = 1 - P = -\sum_{i\geqslant 1} P_i z^i$. The Taylor expansion of $\log(1 - F(z^k))$ in (2.2.12) yields

$$R = P - I = 1 + \sum_{i\geqslant 2}\frac{F^i}{i} + \sum_{k\geqslant 2}\frac{\mu(k)}{k}\sum_{i\geqslant 1}\frac{F(z^k)^i}{i}. \tag{2.2.20}$$

	i	summands	summands with largest degree in $\mathbf{q}$
$[z^n]F^i$	2	$P_j P_{n-j}$, $1 \leqslant j \leqslant n/2$	P_1P_{n-1}, P_2P_{n-2}, P_3P_{n-3} (for $n \geqslant 6$)
	$\geqslant 3$	$P_{j_1}P_{j_2}\cdots P_{j_i}$, $1 \leqslant j_1 \leqslant j_2 \leqslant \cdots \leqslant j_i \leqslant n$, $j_1+j_2+\cdots+j_i = n$,	$P_1^2P_{n-2}$
$[z^n]F(z^k)^i$	1	$P_{n/k}$	$P_{n/k}$
	$\geqslant 2$	$P_{j_1}P_{j_2}\cdots P_{j_i}$, $1 \leqslant j_1 \leqslant j_2 \leqslant \cdots \leqslant j_i \leqslant n/k$, $j_1+j_2\cdots+j_i = n/k$,	$P_1P_{n/k-1}$

Table 2.2.21: Summands of R and bounds on their degrees in $\mathbf{q}$.

Since $R_n = [z^n]R$, we find $R_0 = 1$, $R_1 = 0$, $R_2 = (P_1^2 + P_1)/2$, and $R_3 = P_2P_1 - (P_1^3 - P_1)/3$. Together with (2.2.10), these imply the claims for $n < 4$.

When $n \geqslant 4$, the contributions to $[z^n]R$ from both sums in (2.2.20) are displayed in Table 2.2.21, distinguishing the smallest possible value for i from the remaining larger ones. The third column lists all summands. We first show that the last column displays the terms of largest degree in their row, and then compare the summands in the last column. The terms of $[z^n]F^i$ are products of i factors

$$P_{j_1}P_{j_2}\cdots P_{j_i}, \quad 1 \leqslant j_1 \leqslant j_2 \leqslant \cdots \leqslant j_i \leqslant n,$$

with $j_1 + j_2 + \cdots + j_i = n$. For $i = 2$, we find

$$\deg_{\mathbf{q}} P_1P_{n-1} > \deg_{\mathbf{q}} P_2P_{n-2} > \deg_{\mathbf{q}} P_jP_{n-j} \tag{2.2.22}$$

for all j with $3 \leqslant j \leqslant n/2$ by Lemma 2.2.13 (ii). For $i \geqslant 3$,

$$\deg_{\mathbf{q}} P_1^2P_{n-2} \geqslant \deg_{\mathbf{q}} P_{j_1}P_{j_2}\cdots P_{j_i}$$

for all admissible values of $j_1, j_2, \ldots, j_i$ by repeated application of Lemma 2.2.13 (i) and a single instance of (ii). Let k divide n. Then $[z^n]F(z^k) = -P_{n/k}$ and $[z^n]\sum_{i\geqslant 2} F(z^k)^i$ has degree $\deg_{\mathbf{q}} P_1P_{n/k-1}$ as shown above for $k = 1$.

We continue the comparison started in (2.2.22) by noting that $\deg_{\mathbf{q}} P_2P_{n-2} > \deg_{\mathbf{q}} P_1^2P_{n-2}$ by Lemma 2.2.13 (i), and $\deg_{\mathbf{q}} P_1^2P_{n-2} \geqslant \deg_{\mathbf{q}} P_jP_{n-j}$ for all $3 \leqslant j \leqslant n/2$ with equality only for $(r, n, j) = (2, 6, 3)$ by Lemma 2.2.13 (iii). Furthermore, since $\deg_{\mathbf{q}} P_1 \geqslant 1$, we have for $k \geqslant 2$

$$\deg_{\mathbf{q}} P_1^2P_{n-2} > \deg_{\mathbf{q}} P_{n-2} \geqslant \deg_{\mathbf{q}} P_{n/k} > \deg_{\mathbf{q}} P_1P_{n/k-1},$$

by Lemma 2.2.13 (i). Therefore, the summands of largest degree in $\mathbf{q}$ are in decreasing order P_1P_{n-1}, P_2P_{n-2}, and $P_1^2P_{n-2}$. For $n = 4$, this leads to

$$\begin{aligned} R_4 &= P_1P_3 + P_2^2/2 - P_1^2P_2(1 + O(\mathbf{q}^{-1})) \\ &= P_1P_3\left(1 + \frac{P_2^2}{2P_1P_3} \cdot \left(1 - \frac{P_1^2}{P_2} \cdot (1 + O(\mathbf{q}^{-1}))\right)\right), \end{aligned}$$

while for $n \geqslant 5$, $(r, n) \neq (2, 6)$ we have

$$\begin{aligned} R_n &= P_1P_{n-1} + P_2P_{n-2} - P_1^2P_{n-2}(1 + O(\mathbf{q}^{-1})) \\ &= P_1P_{n-1}\left(1 + \frac{P_2P_{n-2}}{P_1P_{n-1}} \cdot \left(1 - \frac{P_1^2}{P_2}(1 + O(\mathbf{q}^{-1}))\right)\right). \end{aligned} \tag{2.2.23}$$

For $(r, n) = (2, 6)$, we have (2.2.23) with $(1/2 + O(\mathbf{q}^{-1}))$ instead of $(1 + O(\mathbf{q}^{-1}))$.

The estimates (2.2.18) and (2.2.19) follow from

$$\begin{aligned} P_1P_{n-1} &= \rho_{r,n}(\mathbf{q})(1 - q^{-b_{r-1,n-1}}), \\ \frac{P_2P_{n-2}}{P_1P_{n-1}} &= q^{-b_{r-1,n-1}+b_{r-1,2}} \frac{1 + O(\mathbf{q}^{-r(r-1)/2})}{1 - q^{-r}}, \text{ and} \\ \frac{P_1^2}{P_2} &= O(\mathbf{q}^{-r(r-1)/2}). \end{aligned}$$

□

Alekseyev (2006) lists $(\#I_{r,n}(\mathbb{F}_q))_{n\geqslant 0}$ as A115457–A115472 in The On-Line Encyclopedia of Integer Sequences, for $2 \leqslant r \leqslant 6$ and prime $q \leqslant 7$.

Bodin (2008, Theorem 7) states (in our notation)

$$1 - \frac{\#I_{r,n}}{\#P_{r,n}} \sim q^{-b_{r-1,n}-r} \frac{1 - q^{-r}}{1 - q^{-1}}.$$

Hou & Mullen (2009) provide results for $\#I_{r,n}(\mathbb{F}_q)$. These do not yield error bounds for the approximation of $\#R_{r,n}(\mathbb{F}_q)$. Bodin (2010) also uses (2.2.3). Without proving the required bounds on the various terms, as in Lemma 2.2.13, he claims a result similar to (2.2.19), but only for values of n that tend to infinity and with an unspecified multiplicative factor $O(1)$ in the place of our $(1 + O(\mathbf{q}^{-r(r-1)/2}))/(1 - \mathbf{q}^{-r})$ in the error term; the latter is independent of n.

Our approach can be described as follows. We start in the usual framework of algebraic combinatorics with a power series, $P = \sum_{n\geqslant 0} P_n z^n$ in our case, with well-known integer coefficients. Then we consider a well-defined series, $I = \sum_{n\geqslant 0} I_n z^n$ in our case, whose coefficients we want to determine. We find a description of P as $f(I)$ and turn this around to get $I = g(P)$, usually by Möbius inversion. For convergent series, we can then apply powerful tools from calculus, such as singularity analysis, to analyze the asymptotic behavior of the coefficients.

Since our series are not convergent, we deviate from the standard approach. The coefficients P_n are rational functions of the field size q. We introduce a variable $\mathbf{q}$ and define a power series $P \in \mathbb{Q}(\mathbf{q})[\![z]\!]$, whose coefficients are rational functions in a variable $\mathbf{q}$, such that $P(q, z) = P$. Then $g(P)$ is well-defined, and we set $I = g(P) \in \mathbb{Q}(\mathbf{q})[\![z]\!]$. Then $[z^n]\, I(q, z) = I_n$. We now estimate the degrees of the terms in $g(P)$. This yields $I = h(\mathbf{q})(1 + O(\mathbf{q}^{-m}))$, with a main contribution $h(\mathbf{q}) \in \mathbb{Q}(\mathbf{q})$ and a relative error $O(\mathbf{q}^{-m})$, which is an unspecified rational function of degree at most $-m$.

Overall, we first have to determine P, I, f, and g, which is often a substantial part of the labor in the standard framework. From then on, our derivation enjoys three advantages.

- No convergence of the power series is required.
- A clean concentration on the degrees of the various contributions, as embodied in Lemmas 2.2.13, 2.4.8, and 2.5.21.
- The degree of a sum of rational functions is bounded by the degree of the summands.

In the standard approach, the bound for a sum as in the third point has to be multiplied by the number of summands. As to the second point, one sometimes sees in the literature a simple claim of what the main contribution is, without argument. It is not clear whether this constitutes a mathematical proof in the usual sense. Since our series are not convergent, the first point is a definitive requirement.

2.3 EXPLICIT BOUNDS FOR REDUCIBLE POLYNOMIALS

> It must be easy [...] to bring out a *double* set of *results*, viz. —1st, the *numerical magnitudes* which are the results of operations performed on *numerical data*. [...] 2ndly, the *symbolical results* to be attached to those numerical results, which symbolical results are not less the necessary and logical consequences of operations performed upon *symbolical data*, than are numerical results when the data are numerical.
> — Augusta Ada Lovelace

We now describe a third approach to counting the reducible polynomials. The derivation is somewhat more involved. The payoff of this additional effort is an explicit relative error bound in Theorem 2.3.3. However, the calculations are sufficiently complicated for us to stop at the first error term. Thus we replace the asymptotic $1 + O(\mathbf{q}^{-r(r-1)/2})$ in Theorem 2.2.16 by $1/(1 - q^{-1})$.

We consider, for integers $1 \leqslant k < n$, the sets

$$R_{r,n,k}(F) = \{g \cdot h \colon g \in P_{r,k}(F), h \in P_{r,n-k}(F)\} \subseteq P_{r,n}(F).$$

For the remainder of this section we restrict ourselves to finite fields $\mathbb{F}_q$, which we omit from the notation. Then

$$\#R_{r,n,k} \leqslant \#P_{r,k} \cdot \#P_{r,n-k} = q^{u(k)} \frac{(1-q^{-b_{r-1,k}})(1-q^{-b_{r-1,n-k}})}{(1-q^{-1})^2}, \tag{2.3.1}$$

with $u(k) = b_{r,k} + b_{r,n-k} - 2$ as in (2.2.14). The asymptotic behavior of this upper bound is dominated by the behavior of $u(k)$. Since $R_{r,n,k} = R_{r,n,n-k}$, we assume without loss of generality $k \leqslant n/2$. From Lemma 2.2.13 (ii), we know that, for any $r, n \geqslant 2$, $u(k)$ is strictly decreasing for $1 \leqslant k \leqslant n/2$. As $u(k)$ takes only integral values for integers k we conclude that

$$\sum_{2 \leqslant k \leqslant n/2} q^{u(k)} < q^{u(2)} \sum_{k \geqslant 0} q^{-k} = \frac{q^{u(2)}}{1-q^{-1}}. \tag{2.3.2}$$

Theorem 2.3.3. *Let $r, q \geqslant 2$, and $\rho_{r,n}$ as in Theorem 2.2.16. We have*

$$\begin{aligned} \#R_{r,0}(\mathbb{F}_q) &= 1, \\ \#R_{r,1}(\mathbb{F}_q) &= 0, \\ \#R_{r,2}(\mathbb{F}_q) &= \frac{\rho_{r,2}(q)}{2} \cdot (1-q^{-r-1}), \\ |\#R_{r,3}(\mathbb{F}_q) - \rho_{r,3}(q)| &= \rho_{r,3}(q) \cdot q^{-r(r-1)/2} \\ &\quad \cdot \frac{1-2q^{-r}+2q^{-2r-1}-q^{-2r-2}}{3(1-q^{-1})} \\ &\leqslant \rho_{r,3}(q) \cdot q^{-r(r-1)/2}, \end{aligned} \tag{2.3.4}$$

and for $n \geqslant 4$

$$\begin{aligned} |\#R_{r,n}(\mathbb{F}_q) - \rho_{r,n}(q)| &\leqslant \rho_{r,n}(q) \cdot \frac{q^{-\binom{r+n-2}{r-1}+r(r+1)/2}}{(1-q^{-1})(1-q^{-r})} \\ &\leqslant \rho_{r,n}(q) \cdot 3q^{-\binom{r+n-2}{r-1}+r(r+1)/2}. \end{aligned} \tag{2.3.5}$$

Proof. For $n < 4$, the claims follow from Theorem 2.2.16. We remark that the fraction on the right-hand side of (2.3.4) is actually bounded by $2/3$. For $n \geqslant 4$, the proof proceeds in three steps. We claim

$$\#R_{r,n} \leqslant \rho_{r,n}(q)\Big(1 + \frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{(1-q^{-1})(1-q^{-r})}\Big), \tag{2.3.6}$$

$$\#I_{r,n} \geqslant \#P_{r,n}\Big(1 - 3q^{-b_{r-1,n}+r}\frac{1-q^{-r}}{1-q^{-1}}\Big), \tag{2.3.7}$$

$$\#R_{r,n} \geqslant \rho_{r,n}(q)\Big(1 - 3q^{-b_{r-1,n-1}+r}\frac{1-q^{-r-1}}{1-q^{-1}}\Big). \tag{2.3.8}$$

We start with the proof of (2.3.6). Using $R_{r,n} = \bigcup_{1 \leqslant k \leqslant n/2} R_{r,n,k}$ and inequality (2.3.1), we have

$$\#R_{r,n} \leqslant \sum_{1 \leqslant k \leqslant n/2} \#R_{r,n,k}$$

$$\leqslant \frac{1}{(1-q^{-1})^2} \sum_{1\leqslant k\leqslant n/2} q^{u(k)}(1-q^{-b_{r-1,k}})(1-q^{-b_{r-1,n-k}})$$
$$< \frac{1}{(1-q^{-1})^2} \sum_{1\leqslant k\leqslant n/2} q^{u(k)}(1-q^{-b_{r-1,k}}).$$

For the sum, (2.3.2) shows

$$\sum_{1\leqslant k\leqslant n/2} q^{u(k)}(1-q^{-b_{r-1,k}}) < q^{u(1)}(1-q^{-r}) + \sum_{2\leqslant k\leqslant n/2} q^{u(k)} \tag{2.3.9}$$
$$< q^{u(1)}(1-q^{-r}) + \frac{q^{u(2)}}{1-q^{-1}}$$
$$= q^{u(1)}(1-q^{-r})\Big(1+\frac{q^{-u(1)+u(2)}}{(1-q^{-1})(1-q^{-r})}\Big).$$

Since $u(1) = b_{r,n-1} + r - 1$ and $-u(1)+u(2) = -b_{r-1,n-1} + b_{r-1,2}$, we conclude that

$$\#R_{r,n} \leqslant \frac{q^{b_{r,n-1}+r-1}(1-q^{-r})}{(1-q^{-1})^2}\Big(1+\frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{(1-q^{-1})(1-q^{-r})}\Big)$$
$$= \rho_{r,n}(q)\Big(1+\frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{(1-q^{-1})(1-q^{-r})}\Big)$$
$$< \rho_{r,n}(q)(1+3q^{-b_{r-1,n-1}+b_{r-1,2}}). \tag{2.3.10}$$

This proves (2.3.6) and we proceed with (2.3.7). Using (2.3.10), we have

$$\#I_{r,n} = \#P_{r,n} - \#R_{r,n}$$
$$\geqslant \#P_{r,n}\Big(1-\rho_{r,n}(q)\frac{1+3q^{-b_{r-1,n-1}+b_{r-1,2}}}{\#P_{r,n}}\Big)$$
$$= \#P_{r,n}\Big(1-q^{-b_{r-1,n}+r}\frac{(1+3q^{-b_{r-1,n-1}+b_{r-1,2}})(1-q^{-r})}{(1-q^{-1})(1-q^{-b_{r-1,n}})}\Big).$$

We observe that the exponent $-b_{r-1,n-1} + b_{r-1,2}$ is decreasing in r and n for $n \geqslant 4$. It is furthermore always negative and hence the fraction $(1+3q^{-b_{r-1,n-1}+b_{r-1,2}})/(1-q^{-b_{r-1,n}})$ is also decreasing in q. Therefore it achieves its maximal value for $n = 4$, $r = 2$ and $q = 2$, yielding $80/31 < 3$ as upper bound and proving (2.3.7). For the last argument, we need (2.3.7) also for $n = 3$; this follows from Theorem 2.2.16.

We conclude with the proof of (2.3.8). The subset $\{g\cdot h\colon g \in P_{r,1}, h \in I_{r,n-1}\} \subset R_{r,n,k}$ has size $\#P_{r,1}\cdot\#I_{r,n-1}$. With (2.3.7), we find

$$\#R_{r,n} \geqslant \#P_{r,1}\cdot\#I_{r,n-1}$$
$$\geqslant q^{b_{r,1}-1}\frac{1-q^{-r}}{1-q^{-1}}\cdot\#P_{r,n-1}\Big(1-3q^{-b_{r-1,n-1}+r}\frac{1-q^{-r}}{1-q^{-1}}\Big)$$

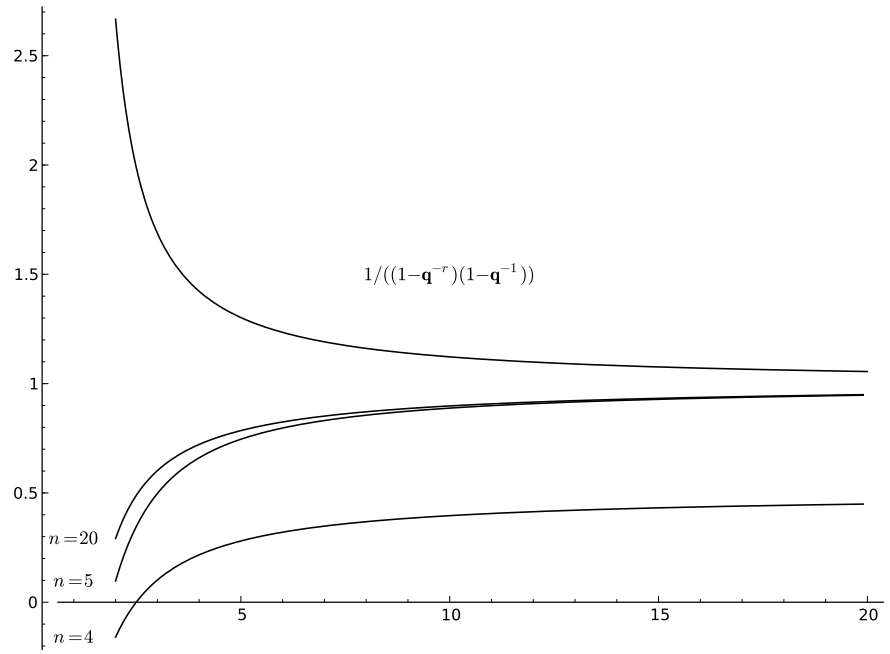

Figure 2.3.11: The normalized relative error in Theorem 2.2.16 for $r = 2$.

$$= \rho_{r,n}(q)(1-q^{-b_{r-1,n-1}})\Big(1-3q^{-b_{r-1,n-1}+r}\frac{1-q^{-r}}{1-q^{-1}}\Big)$$
$$\geqslant \rho_{r,n}(q)\Big(1-3q^{-b_{r-1,n-1}+r}\frac{1-q^{-r-1}}{1-q^{-1}}\Big).$$

We combine the upper and lower bounds (2.3.6) and (2.3.8). The maximum of the bounds on the relative error term is

$$\max\Big(3q^{-r(r-1)/2}(1-q^{-r-1}), \frac{1}{1-q^{-r}}\Big)\cdot\frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{1-q^{-1}}$$
$$= \frac{q^{-\binom{r+n-2}{r-1}+r(r+1)/2}}{(1-q^{-1})(1-q^{-r})}$$

and the observation $(1-q^{-1})(1-q^{-r}) \leqslant 8/3$ concludes the proof. □

The approach of this section also works, with minor modifications, for $n < 4$ and can provide a stand-alone proof of Theorem 2.3.3, without recourse to Theorem 2.2.16.

Figure 2.3.11 shows plots of the normalized relative error $(R_n(\mathbf{q}) - \rho_{r,n}(\mathbf{q}))/(\rho_{r,n}(\mathbf{q})\mathbf{q}^{-\binom{r+n-2}{r-1}+r(r+1)/2})$ for $r = 2$ and $n = 4, 5, 20$ as we substitute for $\mathbf{q}$ real numbers from 2 to 20. Theorem 2.3.3 says that the values are absolutely at most $1/((1-\mathbf{q}^{-r})(1-\mathbf{q}^{-1}))$. Theorem 2.2.16 indicates a bound of $1/2 + o(1)$ for $n = 4$ and $1 + o(1)$ for $n > 4$, but without explicit error estimate.

According to (2.3.5), the bound on the absolute value of the relative error for $n \geqslant 4$ is

$$\frac{q^{-b_{r-1,n-1}+b_{r-1,2}}}{(1-q^{-1})(1-q^{-r})}.$$

For $n > 4$, this is at most $2/3$. For $n = 4$, we can drop the factor $1 - q^{-1}$, since the sum in (2.3.9) consists only of a single summand and the estimate by a geometric sum is not necessary. This shows that also for $n = 4$, the relative error is at most $2/3$.

Remark 2.3.12. How close is our relative error estimate to being exponentially decaying in the input size? The usual dense representation of a polynomial in r variables and of degree n requires $b_{r,n} = \binom{r+n}{r}$ monomials, each of them equipped with a coefficient from $\mathbb{F}_q$, using about $\log_2 q$ bits. Thus the total input size is about $\log_2 q \cdot b_{r,n}$ bits. This differs from $\log_2 q \cdot (b_{r-1,n-1} - b_{r-1,2})$ by a factor of

$$\frac{b_{r,n}}{b_{r-1,n-1} - b_{r-1,2}} < \frac{b_{r,n}}{\frac{1}{2} b_{r-1,n-1}} = \frac{2(n+r)(n+r-1)}{nr}.$$

Up to this polynomial difference (in the exponent), the relative error is exponentially decaying in the bit size of the input, that is, $(\log q)$ times the number of coefficients in the usual dense representation. In particular, it is exponentially decaying in any of the parameters r, n, and $\log_2 q$, when the other two are fixed.

These bounds fit well into the picture described in Section 2 of von zur Gathen (2008) for $r = 2$. The family of functions described there approximates the quotient $\#R_{2,n}/\#P_{2,n}$ (using our notation). If we compare them to $\rho_{r,2}(q)/\#P_{2,n}$ we find that they differ only by the factor $1 - q^{-n-1}$, which tends to 1 as n and q increase. Our bound $3q^{-n+3}$ on the relative error for $r = 2$ and $n \geqslant 4$ is only slightly larger than the bound $2q^{-n+3}$ in Theorem 2.1(ii) of the paper cited.

The following provides some handy bounds.

Corollary 2.3.13. *For $r, q \geqslant 2$, and $n \geqslant 5$, we have*

$$\frac{1}{4} q^{\binom{r+n-1}{r}+r-1} \leqslant \#R_{r,n}(\mathbb{F}_q) \leqslant 6q^{\binom{r+n-1}{r}+r-1},$$
$$\frac{1}{4} q^{-\binom{r+n-1}{r-1}+r} \leqslant \frac{\#R_{r,n}(\mathbb{F}_q)}{\#P_{r,n}(\mathbb{F}_q)} \leqslant 3q^{-\binom{r+n-1}{r-1}+r}.$$

We conclude this section with bounds for the number of irreducible polynomials.

Corollary 2.3.14. *Let $r, q \geqslant 2$, and $\rho_{r,n}$ as in Theorem 2.2.16. We have*

$$\#P_{r,n}(\mathbb{F}_q) - 2\rho_{r,n}(q) \leqslant \#I_{r,n}(\mathbb{F}_q) \leqslant \#P_{r,n}(\mathbb{F}_q), \tag{2.3.15}$$

and more precisely

$$\#I_{r,1}(\mathbb{F}_q) = \#P_{r,1}(\mathbb{F}_q),$$

$$\#\mathrm{I}_{r,2}(\mathbb{F}_q) = \#\mathrm{P}_{r,2}(\mathbb{F}_q) - \frac{\rho_{r,2}(q)}{2} \cdot (1 - q^{-r-1}),$$
$$|\#\mathrm{I}_{r,3}(\mathbb{F}_q) - (\#\mathrm{P}_{r,3}(\mathbb{F}_q) - \rho_{r,3}(q))| \leqslant \rho_{r,3}(q) \cdot q^{-(r-1)r/2},$$

and for $n \geqslant 4$

$$|\#\mathrm{I}_{r,n}(\mathbb{F}_q) - (\#\mathrm{P}_{r,n}(\mathbb{F}_q) - \rho_{r,n}(q))| \leqslant \rho_{r,n}(q) \cdot 3q^{-\binom{r+n-2}{r-1}+r(r+1)/2}.$$

Proof. The more precise statements follow directly from Theorem 2.3.3 by application of $\#\mathrm{P}_{r,n}(\mathbb{F}_q) = \#\mathrm{R}_{r,n}(\mathbb{F}_q) + \#\mathrm{I}_{r,n}(\mathbb{F}_q)$. These imply the first claim for $n < 4$. For $n \geqslant 4$, the relative error in (2.3.5) is at most $2/3 < 1$ as remarked after the proof of Theorem 2.3.3 and this concludes the proof of (2.3.15). □

2.4 POWERFUL POLYNOMIALS

> Writing is nature's way of letting you know how sloppy your thinking is.
> — Dick Guindon
>
> Mathematics is nature's way of letting you know how sloppy your writing is.
> — Leslie Lamport

For an integer $s \geqslant 2$, a polynomial is called *s-powerful* if it is divisible by the s-th power of some nonconstant polynomial, and *s-powerfree* otherwise; it is *squarefree* if $s = 2$. Let

$$\mathrm{Q}_{r,n,s}(F) = \{f \in \mathrm{P}_{r,n}(F) \colon f \text{ is } s\text{-powerful}\},$$
$$\mathrm{S}_{r,n,s}(F) = \mathrm{P}_{r,n}(F) \setminus \mathrm{Q}_{r,n,s}(F).$$

As in the previous section, we restrict our attention to a finite field $F = \mathbb{F}_q$, which we omit from the notation.

For the approach by generating functions, we consider the combinatorial classes $\mathcal{Q} = \bigcup_{n \geqslant 0} \mathrm{Q}_{r,n,s}$ and $\mathcal{S} = \mathcal{P} \setminus \mathcal{Q}$, where the explicit reference to r and s is omitted. Any monic polynomial f factors uniquely as $f = g \cdot h^s$ where g is a monic s-powerfree polynomial and h an arbitrary monic polynomial, hence

$$\mathrm{P} = \mathrm{S} \cdot \mathrm{P}(z^s) \tag{2.4.1}$$

and by definition $\mathrm{Q} = \mathrm{P} - \mathrm{S}$ for the generating functions of $\mathcal{S}$ and $\mathcal{Q}$, respectively. For univariate polynomials, Carlitz (1932) derives (2.4.1) directly from generating functions to prove the counting formula which we reproduce in (2.4.6). Flajolet, Gourdon & Panario (2001, Section 1.1) use (2.4.1) for $s = 2$ to count univariate squarefree polynomials, see also Flajolet & Sedgewick (2009, Note I.66). A corresponding Maple program to compute the coefficients of Q is shown

n	$\#Q_{2,n,3}(\mathbb{F}_q)$
0, 1, 2	0
3	q^2+q
4	$q^4+2q^3+q^2$
5	$q^7+2q^6+2q^5+q^4$
6	$q^{11}+2q^{10}+2q^9+2q^8+q^7+q^5-q^3-q^2$
7	$q^{16}+2q^{15}+2q^{14}+2q^{13}+2q^{12}+q^{11}+q^7+q^6-q^5-2q^4-q^3$
8	$q^{22}+2q^{21}+2q^{20}+2q^{19}+2q^{18}+2q^{17}+q^{16}+q^{10}+q^9-2q^7-2q^6-q^5$
9	$q^{29}+2q^{28}+2q^{27}+2q^{26}+2q^{25}+2q^{24}+2q^{23}+q^{22}+q^{14}+q^{13}-q^{11}-2q^{10}-q^9-q^7-2q^6-q^5+q^4+q^3$

n	$\#Q_{3,n,2}(\mathbb{F}_q)$
0, 1	0
2	q^3+q^2+q
3	$q^6+2q^5+3q^4+2q^3+q^2$
4	$q^{12}+2q^{11}+3q^{10}+4q^9+4q^8+4q^7+2q^6-2q^4-2q^3-q^2$
5	$q^{22}+2q^{21}+3q^{20}+3q^{19}+3q^{18}+3q^{17}+3q^{16}+3q^{15}+3q^{14}+3q^{13}+3q^{12}+3q^{11}+3q^{10}+2q^9-3q^7-5q^6-5q^5-3q^4-q^3$
6	$q^{37}+2q^{36}+3q^{35}+3q^{34}+3q^{33}+3q^{32}+3q^{31}+3q^{30}+3q^{29}+3q^{28}+3q^{27}+3q^{26}+3q^{25}+3q^{24}+3q^{23}+2q^{22}+q^{21}+q^{19}+2q^{18}+3q^{17}+4q^{16}+4q^{15}+3q^{14}+q^{13}-4q^{12}-8q^{11}-11q^{10}-11q^9-8q^8-3q^7+2q^6+4q^5+3q^4+q^3$

n	$\#Q_{3,n,3}(\mathbb{F}_q)$
0, 1, 2	0
3	q^3+q^2+q
4	$q^6+2q^5+3q^4+2q^3+q^2$
5	$q^{12}+2q^{11}+3q^{10}+3q^9+3q^8+3q^7+2q^6+q^5$
6	$q^{22}+2q^{21}+3q^{20}+3q^{19}+3q^{18}+3q^{17}+3q^{16}+3q^{15}+3q^{14}+3q^{13}+2q^{12}+q^{11}+q^9+q^8+q^7-q^5-2q^4-2q^3-q^2$
7	$q^{37}+2q^{36}+3q^{35}+3q^{34}+3q^{33}+3q^{32}+3q^{31}+3q^{30}+3q^{29}+3q^{28}+3q^{27}+3q^{26}+3q^{25}+3q^{24}+3q^{23}+2q^{22}+q^{21}+q^{12}+2q^{11}+3q^{10}+2q^9-3q^7-5q^6-5q^5-3q^4-q^3$

Table 2.4.3: Exact values of $\#Q_{r,n,s}(\mathbb{F}_q)$ for small values of r, n, s.

```
spowerfreesGF:=proc(z,N,r,s) local i: option remember:
    convert(taylor(allpolysGF(z,N,r)/allpolysGF(z^s,N,r),
        z,N+1),polynom):
end:

spowerfulsGF:=proc(z,N,r,s) option remember:
    allpolysGF(z,N,r)-spowerfreesGF(z,N,r,s):
end:

spowerfuls:=proc(n,r,s)
    coeff(sort(expand(spowerfulsGF(z,n,r,s))),z^n):
end:
```

Figure 2.4.2: Maple program to compute the number of monic s-powerful polynomials in r variables of degree n.

in Figure 2.4.2. It was used to compute $\#Q_{2,n,2}(\mathbb{F}_q)$ for $n \leqslant 6$ in von zur Gathen (2008, Table 3.1). We extend this in Table 2.4.3.

As in Theorem 2.2.7, this approach quickly leads to explicit formulas.

Theorem 2.4.4. *For $r \geqslant 1$, $q, s \geqslant 2$, P_n as in* (2.2.1)*, and M_n as in* (2.2.6)*, we have*

$$S_n = \sum_{\substack{0 \leqslant i \leqslant n/s \\ j \in M_i}} (-1)^{|j|} P_{j_1} P_{j_2} \cdots P_{j_{|j|}} P_{n-is},$$

$$Q_n = -\sum_{\substack{1 \leqslant i \leqslant n/s \\ j \in M_i}} (-1)^{|j|} P_{j_1} P_{j_2} \cdots P_{j_{|j|}} P_{n-is}. \tag{2.4.5}$$

Proof. We consider the original power series $F = 1 - P = -\sum_{i \geqslant 1} P_i z^i$ and express (2.4.1) as

$$\begin{aligned} S &= P \cdot \sum_{i \geqslant 0} F(z^s)^i \\ &= \sum_{k \geqslant 0} P_k z^k \cdot \sum_{i \geqslant 0} \Big(-\sum_{j \geqslant 1} P_j z^{js} \Big)^i. \end{aligned}$$

Comparison of coefficients provides us with

$$S_n = \sum_{\substack{0 \leqslant i \leqslant n/s \\ j \in M_i}} (-1)^{|j|} P_{j_1} P_{j_2} \cdots P_{j_{|j|}} P_{n-is},$$

and the claim for $Q_n = P_n - S_n$ follows. □

For $r = 1$, we have $P_j = q^j$ and for any composition $j_1 + j_2 + \cdots + j_k$ of i in (2.4.5)

$$P_{j_1} P_{j_2} \cdots P_{j_k} P_{n-is} = q^{n-(s-1)i}.$$

Moreover, since

$$\sum_{k\geqslant 1}(-1)^k\binom{i-1}{k-1} = -\binom{0}{i-1} = \begin{cases} -1 & \text{if } i=1,\\ 0 & \text{if } i\geqslant 2,\end{cases}$$

see Graham, Knuth & Patashnik (1989, p. 167), we have in the univariate case

$$Q_n = -\sum_{\substack{1\leqslant i\leqslant n/s\\ k\geqslant 1}}(-1)^k\binom{i-1}{k-1}q^{n-(s-1)i} = \begin{cases} 0 & \text{if } n<s,\\ q^{n-s+1} & \text{if } n\geqslant s,\end{cases} \tag{2.4.6}$$

as shown by Carlitz (1932, Section 6).

To study the asymptotic behavior of S_n and Q_n for $r \geqslant 2$ we again deviate from the standard approach and move to power series in $\mathbb{Q}(\mathbf{q})[\![z]\!]$. With P from (2.2.11), we define $S, Q \in \mathbb{Q}(\mathbf{q})[\![z]\!]$ by

$$\begin{aligned} P &= S\cdot P(z^s),\\ Q &= P - S.\end{aligned}$$

This is well-defined, since $P(z^s)$ has constant term 1 and is therefore invertible. By construction, we have

$$\begin{aligned} S_n(q) &= \#S_{r,n,s}(\mathbb{F}_q),\\ Q_n(q) &= \#Q_{r,n,s}(\mathbb{F}_q).\end{aligned}$$

To study the asymptotic behavior, we examine $P_k\cdot P_{n-sk}$. Let

$$\begin{aligned} \nu_{r,n,s}(k) &= \deg_{\mathbf{q}}(P_k\cdot P_{n-sk})\\ &= (r+k)^{\underline{r}}/r! + (r+n-sk)^{\underline{r}}/r! - 2\end{aligned}$$

and consider $\nu_{r,n,s}(k)$ as a function of a real variable k (Figure 2.4.7). In contrast to $u(k)$ from Section 2.2, this function is not monotone in k.

Lemma 2.4.8. *Let* $r, n, s, q \geqslant 2$.

(i) The function $\nu_{r,n,s}(k)$ *is convex for* $1 \leqslant k \leqslant n/s$.

(ii) For all integers k *with* $2 \leqslant k \leqslant n/s$, *we have*

$$\nu_{r,n,s}(1) > \nu_{r,n,s}(k).$$

(iii) For all integers k *with* $3 \leqslant k \leqslant n/s$, *we have*

$$\nu_{r,n,s}(2) > \nu_{r,n,s}(k) \qquad \text{if } (n,s)\neq(6,2).$$

Furthermore,

$$\begin{aligned} &\nu_{r,6,2}(2) < \nu_{r,6,2}(3) && \text{if } r\geqslant 3,\\ &\nu_{2,6,2}(2) = \nu_{2,6,2}(3)+1.\end{aligned}$$

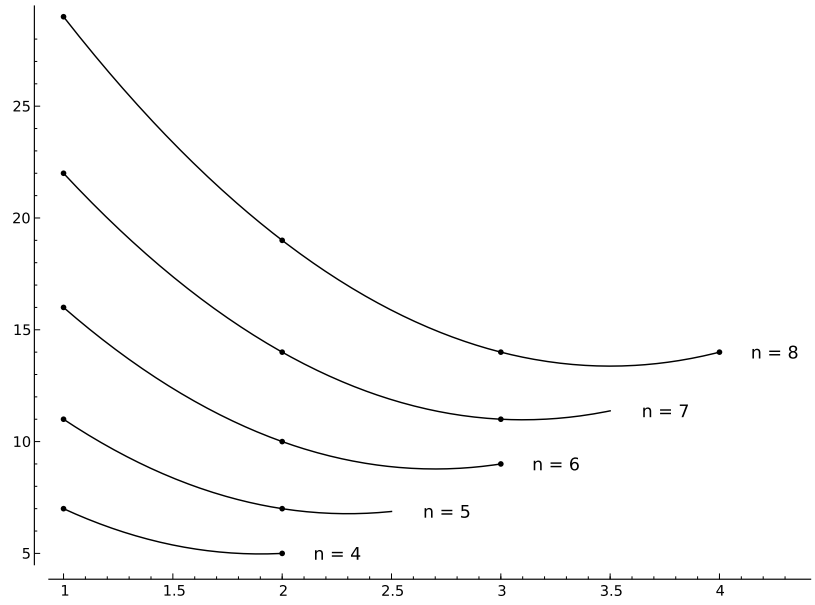

Figure 2.4.7: Graphs of $\nu_{2,n,2}(k)$ on $[1, n/2]$ as n runs from 4 to 8. The dots represent the values at integer arguments.

(iv) If $(n, s) \neq (6, 2)$, *then*

$$\sum_{2 \leqslant k \leqslant n/s} q^{\nu_{r,n,s}(k)} \leqslant \frac{2q^{\nu_{r,n,s}(2)}}{1 - q^{-1}}.$$

Proof. We switch to the affine transformation

$$\begin{aligned} \bar{\nu}(k) &= r! \cdot \Big(\nu_{r,n,s}(k) + 2 \Big) \\ &= (r+k)^{\underline{r}} + (r+n-sk)^{\underline{r}}, \end{aligned}$$

which exhibits the same behavior as $\nu_{r,n,s}$ concerning convexity and maximality.

(i) We have

$$\bar{\nu}''(k) = \sum_{\substack{1 \leqslant i,j \leqslant r \\ i \neq j}} \Big(\frac{(r+k)^{\underline{r}}}{(i+k)(j+k)} + \frac{s^2 (r+n-sk)^{\underline{r}}}{(i+n-sk)(j+n-sk)} \Big) > 0.$$

(ii) For $n < 2s$, there is nothing to prove. For $n \geqslant 2s$, we find $n \geqslant s+2 \geqslant s+1+1/(s-1)$ and for all i

$$\begin{aligned} (i+n-s) - (i+n/s) &\geqslant 0, \\ (r+n-s)^{\underline{r}} - (r+n/s)^{\underline{r}} &\geqslant 0, \\ \bar{\nu}(1) - \bar{\nu}(n/s) = (r+1)! + (r+n-s)^{\underline{r}} - (r+n/s)^{\underline{r}} - r! \\ = (r+n-s)^{\underline{r}} - (r+n/s)^{\underline{r}} + r \cdot r! > 0. \end{aligned}$$

With the convexity of $\bar{\nu}$, this suffices.

(iii) Analogously to (ii), it is sufficient to prove $\bar{\nu}(2) > \bar{\nu}(n/s)$ for $(n,s) \neq (6,2)$. If $n \geqslant 2s^2/(s-1)$, then $n - 2s \geqslant n/s$, so that for all i

$$(i + n - 2s) - (i + n/s) \geqslant 0$$

and hence

$$\begin{aligned}\bar{\nu}(2) - \bar{\nu}(n/s) &= (r+2)!/2 + (r+n-2s)^{\underline{r}} - (r+n/s)^{\underline{r}} - r! \\ &> (r+n-2s)^{\underline{r}} - (r+n/s)^{\underline{r}} \geqslant 0.\end{aligned}$$

If $n < 2s^2/(s-1)$, then $n/s < 3$ for $s \geqslant 3$ or $n < 6$ and there is nothing to prove. Finally, the three conditions $n < 2s^2/(s-1)$, $s = 2$, and $n \geqslant 6$ enforce $6 \leqslant n < 8$, and we compute directly

$$\nu_{r,7,2}(2) - \nu_{r,7,2}(3) = \frac{1}{2} r(r+1) > 0,$$

$$\nu_{r,6,2}(2) - \nu_{r,6,2}(3) = -\frac{1}{6}(r-3)(r+1)(r+2) - 1 \begin{cases} = 1 & \text{if } r = 2, \\ < 0 & \text{if } r \geqslant 3. \end{cases}$$

(iv) The maximal value of the integer sequence $\nu_{r,n,s}(k)$ for $2 \leqslant k \leqslant n/s$ is $\nu_{r,n,s}(2)$ by (iii). Each value is taken at most twice, due to (i), and we can bound the sum by twice a geometric sum as

$$\sum_{2 \leqslant k \leqslant n/s} q^{\nu_{r,n,s}(k)} \leqslant 2q^{\nu_{r,n,s}(2)} \sum_{k \geqslant 0} q^{-k} = \frac{2q^{\nu_{r,n,s}(2)}}{1 - q^{-1}}. \quad \square$$

The approach by generating functions now yields the following result. Its "general" case is (iv). We give exact expressions in special cases, namely for $n < 3s$ in (ii) and for $(n,s) = (6,2)$ in (iii), which also apply when we substitute the size q of a finite field $\mathbb{F}_q$ for $\mathbf{q}$.

Theorem 2.4.9. *Let* $r, s \geqslant 2$, $n \geqslant 0$, *and*

$$\eta_{r,n,s}(\mathbf{q}) = \mathbf{q}^{\binom{r+n-s}{r}+r-1} \frac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-\binom{r+n-s-1}{r-1}})}{(1-\mathbf{q}^{-1})^2} \in \mathbb{Q}(\mathbf{q}),$$

$$\delta = \binom{r+n-s}{r} - \binom{r+n-2s}{r} - \frac{r(r+1)}{2}.$$

(i) If $n \geqslant 2s$, *then* $\delta \geqslant r$.

(ii)

$$Q_n = \begin{cases} 0 & \text{for } n < s, \\ \eta_{r,n,s}(\mathbf{q}) & \text{for } s \leqslant n < 2s, \\ \eta_{r,n,s}(\mathbf{q}) \Big(1 + \mathbf{q}^{-\delta} \cdot \frac{1-\mathbf{q}^{-\binom{n+r-2s-1}{r-1}}}{1-\mathbf{q}^{-\binom{n+r-s-1}{r-1}}} & \\ \quad \cdot \Big(\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-r}} - \mathbf{q}^{-r(r-1)/2} \frac{1-\mathbf{q}^{-r}}{1-\mathbf{q}^{-1}} \Big) \Big) & \text{for } 2s \leqslant n < 3s. \end{cases} \tag{2.4.10}$$

(iii) For $(n,s)=(6,2)$ *and* $r\geqslant 2$, *we have*

$$\begin{aligned}Q_6 &= \eta_{r,6,2}(\mathbf{q})\Bigg(1+\mathbf{q}^{-\binom{r+3}{4}-r+1}\cdot\Big(\mathbf{q}^{-1}\frac{(1-\mathbf{q}^{-1})\big(1-\mathbf{q}^{-\binom{r+2}{3}}\big)}{(1-\mathbf{q}^{-r})\big(1-\mathbf{q}^{-\binom{r+3}{4}}\big)}\\
&\quad+\mathbf{q}^{-(r^3-7r+6)/6}\frac{(1-\mathbf{q}^{-r(r+1)/2})^2}{(1-\mathbf{q}^{-r})\big(1-\mathbf{q}^{-\binom{r+3}{4}}\big)}\\
&\quad-\mathbf{q}^{-(r^3+3r^2-10r+6)/6}\frac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-r(r+1)/2})}{(1-\mathbf{q}^{-1})\big(1-\mathbf{q}^{-\binom{r+3}{4}}\big)}\\
&\quad-2\mathbf{q}^{-(r^3+3r^2+4r-6)/6}\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-\binom{r+3}{4}}}\\
&\quad+\mathbf{q}^{-(r^3+6r^2-7r+6)/6}\frac{(1-\mathbf{q}^{-r})^2}{(1-\mathbf{q}^{-1})\big(1-\mathbf{q}^{-\binom{r+3}{4}}\big)}\Big)\Bigg)\\
&=\eta_{r,6,2}(\mathbf{q})\big(1+\mathbf{q}^{-\delta+(r-2)(r-1)(r+3)/6}(1+O(\mathbf{q}^{-1}))\big).\end{aligned}\tag{2.4.11}$$

(iv) For $n\geqslant 2s$ *and* $(n,s)\neq(6,2)$, *we have*

$$Q_n=\eta_{r,n,s}(\mathbf{q})\big(1+\mathbf{q}^{-\delta}(1+O(\mathbf{q}^{-1}))\big).\tag{2.4.12}$$

Proof. (i) If $n\geqslant 2s$, then

$$\delta\geqslant\binom{r+s}{r}-1-\frac{r(r+1)}{2}\geqslant\binom{r+2}{r}-1-\frac{r(r+1)}{2}=r.$$

(ii) The exact formulas of Theorem 2.4.4 yield

$$\begin{aligned}&Q_n=0 && \text{for } n<s,\\ &Q_n=P_1P_{n-s}=\eta_{r,n,s}(\mathbf{q}) && \text{for } s\leqslant n<2s,\end{aligned}$$

and for $2s\leqslant n<3s$,

$$\begin{aligned}S_n &= P_n-P_1P_{n-s}-(P_2-P_1^2)P_{n-2s},\\
Q_n &= P_1P_{n-s}+(P_2-P_1^2)P_{n-2s}\\
&=\eta_{r,n,s}(\mathbf{q})\Big(1+\frac{P_2P_{n-2s}}{P_1P_{n-s}}\Big(1-\frac{P_1^2}{P_2}\Big)\Big)\\
&=\eta_{r,n,s}(\mathbf{q})\Bigg(1+\mathbf{q}^{-\delta}\frac{1-\mathbf{q}^{-\binom{n+r-2s-1}{r-1}}}{1-\mathbf{q}^{-\binom{n+r-s-1}{r-1}}}\\
&\qquad\cdot\Big(\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-r}}-\mathbf{q}^{-r(r-1)/2}\frac{1-\mathbf{q}^{-r}}{1-\mathbf{q}^{-1}}\Big)\Bigg),\end{aligned}\tag{2.4.13}$$

where $\delta=-\deg_{\mathbf{q}}(P_2P_{n-2s}/(P_1P_{n-s}))$.

(iii) For $s=2$, we evaluate (2.4.5) for

$$\begin{aligned}Q_6 &= P_1P_4+P_3+P_2^2-P_1^2P_2-2P_1P_2+P_1^3\\
&=\eta_{r,6,2}(\mathbf{q})(1+(P_3+P_2^2-P_1^2P_2-2P_1P_2+P_1^3)/(P_1P_4))\end{aligned}$$

$$
\begin{aligned}
&= \eta_{r,6,2}(\mathbf{q})\Bigg(1 + \mathbf{q}^{-\nu_{r,6,2}(1)+\nu_{r,6,2}(3)+1} \\
&\quad \cdot \Big(\mathbf{q}^{-1}\tfrac{(1-\mathbf{q}^{-1})(1-\mathbf{q}^{-b_{r-1,3}})}{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-b_{r-1,4}})} && (2.4.14)\\
&\quad + \mathbf{q}^{-(r^3-7r+6)/6}\tfrac{(1-\mathbf{q}^{-r(r+1)/2})^2}{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-b_{r-1,4}})} \\
&\quad - \mathbf{q}^{-(r^3+3r^2-10r+6)/6}\tfrac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-r(r+1)/2})}{(1-\mathbf{q}^{-1})(1-\mathbf{q}^{-b_{r-1,4}})} \\
&\quad - 2\mathbf{q}^{-(r^3+3r^2+4r-6)/6}\tfrac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-b_{r-1,4}}} \\
&\quad + \mathbf{q}^{-(r^3+6r^2-7r+6)/6}\tfrac{(1-\mathbf{q}^{-r})^2}{(1-\mathbf{q}^{-1})(1-\mathbf{q}^{-b_{r-1,4}})}\Big)\Bigg) && (2.4.15)\\
&= \eta_{r,6,2}(\mathbf{q})\big(1 + \mathbf{q}^{-\delta+(r-2)(r-1)(r+3)/6}(1 + O(\mathbf{q}^{-1}))\big), && (2.4.16)
\end{aligned}
$$

since the sum (2.4.14)–(2.4.15) has nonpositive degree in $\mathbf{q}$ and $-\nu_{r,6,2}(1) + \nu_{r,6,2}(3) + 1 = -\binom{r+3}{4} - r + 1 = -\delta + (r-2)(r-1)(r+3)/6$.

(iv) Finally, for $n \geqslant 2s$ and $(n,s) \neq (6,2)$, we claim

$$S_n = P_n - P_1 P_{n-s} - P_2 P_{n-2s}(1 + O(\mathbf{q}^{-1})). \tag{2.4.17}$$

This implies immediately

$$
\begin{aligned}
S_n &= P_n - P_1 P_{n-s}(1 + O(\mathbf{q}^{-1})) \\
&= P_n(1 + O(\mathbf{q}^{-1})),
\end{aligned} \tag{2.4.18}
$$

by Lemmas 2.4.8 (ii) and 2.2.13 (i), respectively. We already have (2.4.17) for $2s \leqslant n < 3s$ from (2.4.13) by Lemma 2.2.13 (i). We also have (2.4.18) for $(n,s) = (6,2)$ from (2.4.16). This is enough to obtain inductively

$$
\begin{aligned}
S_n &= P_n - \sum_{1 \leqslant i \leqslant n/s} S_{n-is} P_i \\
&= P_n - P_1 S_{n-s} - \sum_{2 \leqslant i \leqslant n/s} P_i S_{n-is} \\
&= P_n - P_1\big(P_{n-s} - P_1 P_{n-2s}(1 + O(\mathbf{q}^{-1}))\big) \\
&\quad - \sum_{2 \leqslant i \leqslant n/s} P_i P_{n-is}(1 + O(\mathbf{q}^{-1})) \\
&= P_n - P_1 P_{n-s} + P_1^2 P_{n-2s}(1 + O(\mathbf{q}^{-1})) \\
&\quad - P_2 P_{n-2s}(1 + O(\mathbf{q}^{-1})) \\
&= P_n - P_1 P_{n-s} - P_2 P_{n-2s}(1 + O(\mathbf{q}^{-1})),
\end{aligned}
$$

using Lemma 2.4.8 (iii) for $(n,s) \neq (6,2)$ and Lemma 2.2.13 (i). We conclude with

$$Q_n = P_1 P_{n-s} + P_2 P_{n-2s}(1 + O(\mathbf{q}^{-1}))$$

$$= \eta_{r,n,s}(\mathbf{q})(1+\mathbf{q}^{-\delta}(1+O(\mathbf{q}^{-1})))$$

by $\eta_{r,n,s}(\mathbf{q}) = P_1 P_{n-s}$ and $\delta = -\deg_{\mathbf{q}}(P_2 P_{n-2s}/(P_1 P_{n-s}))$, respectively. □

For $r \geqslant 3$, we can replace $1+O(\mathbf{q}^{-1})$ in (2.4.11) by $\mathbf{q}^{-1}+O(\mathbf{q}^{-2})$.

In the following, the combinatorial approach replaces the asymptotic $1+O(\mathbf{q}^{-1})$ of (2.4.12) with an explicit bound of 6 in (2.4.22). We consider for integers $1 \leqslant k \leqslant n/s$ the sets

$$Q_{r,n,s,k}(F) = \{g \cdot h^s : g \in P_{r,n-sk}, h \in P_{r,k}\} \in P_{r,n}(F)$$

and have

$$Q_{r,n,s}(F) = \bigcup_{1 \leqslant k \leqslant n/s} Q_{r,n,s,k}(F). \tag{2.4.19}$$

For $n < 3s$ the exact formula (2.4.10) of Theorem 2.4.9 (ii) applies. We provide explicit bounds for $n \geqslant 3s$.

Theorem 2.4.20. *Let* $r, s, q \geqslant 2$, $n \geqslant 0$, *and*

$$\eta_{r,n,s}(\mathbf{q}) = \mathbf{q}^{\binom{r+n-s}{r}+r-1} \frac{(1-\mathbf{q}^{-r})\left(1-\mathbf{q}^{-\binom{r+n-s-1}{r-1}}\right)}{(1-\mathbf{q}^{-1})^2} \in \mathbb{Q}(\mathbf{q}),$$
$$\delta = \binom{r+n-s}{r} - \binom{r+n-2s}{r} - \frac{r(r+1)}{2}$$

as in Theorem 2.4.9.

(i) For $(n,s) = (6,2)$, *we have* $\delta = r(r+1)(r^2+9r+2)/24$ *and*

$$|\#Q_{r,6,2}(\mathbb{F}_q) - \eta_{r,6,2}(q)| \leqslant \eta_{r,6,2}(q) \cdot 2q^{-\delta+(r-2)(r-1)(r+3)/6}. \tag{2.4.21}$$

(ii) For $n \geqslant 3s$ *and* $(n,s) \neq (6,2)$, *we have*

$$|\#Q_{r,n,s}(\mathbb{F}_q) - \eta_{r,n,s}(q)| \leqslant \eta_{r,n,s}(q) \cdot 6q^{-\delta}. \tag{2.4.22}$$

Proof. We omit the argument $\mathbb{F}_q$ from the notation. Considering only the positive and negative summands of (2.4.15), respectively, we find

$$\#Q_{r,6,2} \leqslant \eta_{r,6,2}(q)(1+2q^{-\delta+(r-2)(r-1)(r+3)/6}), \tag{2.4.23}$$
$$\#Q_{r,6,2} \geqslant \eta_{r,6,2}(q)(1-q^{-\delta+(r-2)(r-1)(r+3)/6}),$$

which proves (i).

For the general case (ii), we claim

$$\#Q_{r,n,s} \leqslant \eta_{r,n,s}(q)\left(1+\frac{16}{3}q^{-\delta}\right) \text{ for } (n,s) \neq (6,2), \tag{2.4.24}$$
$$\#Q_{r,n,s} \geqslant \eta_{r,n,s}(q)\left(1-\frac{7}{2}q^{-\delta-r(r-1)/2}\right) \text{ for } n \geqslant 3s. \tag{2.4.25}$$

For (2.4.24), we find from (2.4.19)

$$\begin{aligned}
\#Q_{r,n,s} &\leqslant \sum_{1\leqslant k\leqslant n/s} \#Q_{r,n,s,k} \leqslant \sum_{1\leqslant k\leqslant n/s} \#P_{r,n-sk}\cdot\#P_{r,k} \\
&= \sum_{1\leqslant k\leqslant n/s} q^{\nu_{r,n,s}(k)}\frac{(1-q^{-b_{r-1,n-sk}})(1-q^{-b_{r-1,k}})}{(1-q^{-1})^2} \\
&= \eta_{r,n,s}(q)\Big(1+q^{-\nu_{r,n,s}(1)} \\
&\quad\cdot \sum_{2\leqslant k\leqslant n/s} q^{\nu_{r,n,s}(k)}\frac{(1-q^{-b_{r-1,k}})(1-q^{-b_{r-1,n-sk}})}{(1-q^{-r})(1-q^{-b_{r-1,n-s}})}\Big) \\
&\leqslant \eta_{r,n,s}(q)\Big(1+q^{-\nu_{r,n,s}(1)}\cdot \sum_{2\leqslant k\leqslant n/s} q^{\nu_{r,n,s}(k)}\frac{(1-q^{-b_{r-1,k}})}{(1-q^{-r})}\Big) \\
&\leqslant \eta_{r,n,s}(q)\Big(1+\frac{2q^{-\nu_{r,n,s}(1)+\nu_{r,n,s}(2)}}{(1-q^{-r})(1-q^{-1})}\Big) \leqslant \eta_{r,n,s}(q)\Big(1+\frac{16}{3}q^{-\delta}\Big),
\end{aligned}$$

using the bound of Lemma 2.4.8 (iv).

To prove (2.4.25), we observe that $Q_{r,n,s,1}$ contains an injective image of $(P_{r,n-s}\setminus Q_{r,n-s,s})\times I_{r,1}$ by $(g,h)\mapsto g\cdot h^s$. For $n\geqslant 3s$, we get from $I_{r,1}=P_{r,1}$

$$\begin{aligned}
\#Q_{r,n,s} &\geqslant \#Q_{r,n,s,1} \\
&\geqslant \#I_{r,1}\cdot\#(P_{r,n-s}\setminus Q_{r,n-s,s}) \\
&\geqslant \#P_{r,1}\cdot(\#P_{r,n-s}-\#Q_{r,n-s,s}) \\
&\geqslant \eta_{r,n,s}(q)\cdot\Big(1-\frac{\eta_{r,n-s,s}(q)(1+\frac{16}{3}q^{-r})}{\#P_{r,n-s}}\Big) \\
&\geqslant \eta_{r,n,s}(q)\cdot\Big(1-q^{b_{r,n-2s}-b_{r,n-s}+r} \\
&\quad\cdot\frac{(1-q^{-r})(1-q^{-b_{r-1,n-2s}})(1+\frac{16}{3}q^{-r})}{(1-q^{-1})(1-q^{-b_{r-1,n-s}})}\Big) \qquad (2.4.26)\\
&\geqslant \eta_{r,n,s}(q)\Big(1-\frac{7}{2}q^{-\delta-r(r-1)/2}\Big),
\end{aligned}$$

if $(n,s)\neq(8,2)$ using (2.4.24) for $Q_{r,n-s,s}$ with exponent $\delta\geqslant r$ by Theorem 2.4.9 (i).

If $(n,s)=(8,2)$, we modify (2.4.26) according to (2.4.23) and get

$$\begin{aligned}
\#Q_{r,8,2} &\geqslant \eta_{r,8,2}(q)\Big(1-\frac{3}{2}\big(1+2q^{-\binom{r+3}{4}-r+1}\big)q^{-\delta-r(r-1)/2}\Big) \\
&\geqslant \eta_{r,8,2}(q)(1-2q^{-\delta-r(r-1)/2}).
\end{aligned}$$

Combining (2.4.24) and (2.4.25) proves (ii). □

We note that for $(n,s)=(6,2)$, inequality (2.4.22) follows from (2.4.21) if $r=2$ and is false for sufficiently large q if $r\geqslant 3$.

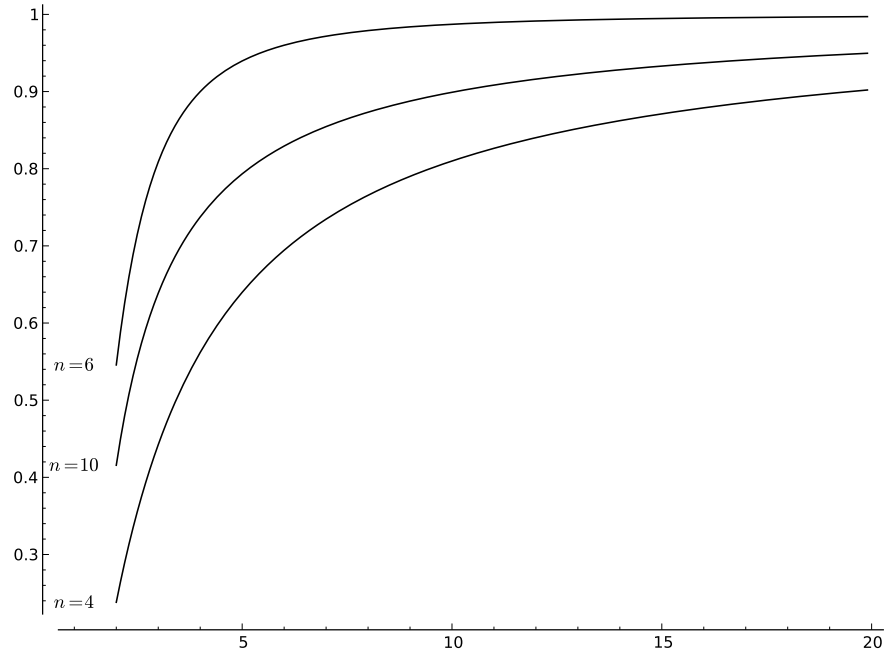

Figure 2.4.27: The normalized relative error in Theorem 2.4.9 (iii)–(iv) for $(r, s) = (2, 2)$.

Figure 2.4.27 shows plots of $(Q_{r,n,s}(\mathbf{q}) - \eta_{r,n,s}(\mathbf{q}))/(\eta_{r,n,s}(\mathbf{q})\mathbf{q}^{-\delta})$ for $r = 2$, $s = 2$ and $n = 4, 6, 10$, as we substitute for $\mathbf{q}$ real numbers from 2 to 20.

Remark 2.4.28. As noted in Remark 2.3.12 for reducible polynomials, the relative error term is (essentially) exponentially decreasing in the input size, and exponentially decaying in any of the parameters r, n, s, and $\log_2 q$, when the other three are fixed.

In the bivariate case, von zur Gathen (2008, Theorem 3.1) approximates the quotient $\#Q_{2,n,s}(\mathbb{F}_q)/\#P_{2,n}(\mathbb{F}_q)$ (using our notation) by

$$q^{-(2ns-s^2+3s-4)/2}\frac{(1+q^{-1})(1-q^{-n+s-1})}{1-q^{-n-1}},$$

which equals the term $\eta_{2,n,s}(q)/\#P_{2,n}(\mathbb{F}_q)$ derived from our analysis above.

We append handy bounds using Corollary 2.3.13.

Corollary 2.4.29. *For $r, s, q \geqslant 2$, and $n \geqslant s$, we have*

$$\begin{aligned}
\frac{1}{2}q^{\binom{r+n-s}{r}+r-1} &\leqslant \#Q_{r,n,s}(\mathbb{F}_q) \leqslant 10q^{\binom{r+n-s}{r}+r-1},\\
\frac{1}{2}q^{-\binom{r+n}{r}+\binom{r+n-s}{r}+r} &\leqslant \frac{\#Q_{r,n,s}(\mathbb{F}_q)}{\#P_{r,n}(\mathbb{F}_q)} \leqslant 5q^{-\binom{r+n}{r}+\binom{r+n-s}{r}+r},\\
\frac{1}{6}q^{-\binom{r+n-1}{r}+\binom{r+n-s}{r}} &\leqslant \frac{\#Q_{r,n,s}(\mathbb{F}_q)}{\#R_{r,n}(\mathbb{F}_q)} \leqslant 19q^{-\binom{r+n-1}{r}+\binom{r+n-s}{r}}.
\end{aligned}$$

We conclude this section with bounds for the number of s-powerfree polynomials.

Corollary 2.4.30. *Let $r, s, q \geqslant 2$, $n \geqslant 0$, and $\eta_{r,n,s}$ and δ as in Theorem 2.4.9. We have*

$$\#P_{r,n}(\mathbb{F}_q) - 3\eta_{r,n,s}(q) \leqslant \#S_{r,n,s}(\mathbb{F}_q) \leqslant \#P_{r,n}(\mathbb{F}_q),$$

and more precisely

$$\#S_{r,n,s}(\mathbb{F}_q) = \begin{cases} \#P_{r,n}(\mathbb{F}_q) & \text{for } n < s, \\ \#P_{r,n}(\mathbb{F}_q) - \eta_{r,n,s}(q) & \text{for } s \leqslant n < 2s, \\ \#P_{r,n}(\mathbb{F}_q) - \eta_{r,n,s}(q)\Big(1 + q^{-\delta} & \\ \quad \cdot \frac{1-q^{-\binom{n+r-2s-1}{r-1}}}{1-q^{-\binom{n+r-s-1}{r-1}}} \cdot \Big(\frac{1-q^{-r(r+1)/2}}{1-q^{-r}} & \text{for } 2s \leqslant n < 3s, \\ \quad -q^{-r(r-1)/2}\frac{1-q^{-r}}{1-q^{-1}}\Big)\Big) & \end{cases}$$

$$|\#S_{r,6,2}(\mathbb{F}_q) - (\#P_{r,n}(\mathbb{F}_q) - \eta_{r,6,2}(q))| \leqslant \eta_{r,6,2}(q) \cdot 2q^{-\delta+(r-2)(r-1)(r+3)/6},$$

and for $n \geqslant 3s$ with $(n, s) \neq (6, 2)$

$$|\#S_{r,n,s}(\mathbb{F}_q) - (\#P_{r,n}(\mathbb{F}_q) - \eta_{r,n,s}(q))| \leqslant \eta_{r,n,s}(q) \cdot 6q^{-\delta}.$$

2.5 RELATIVELY IRREDUCIBLE POLYNOMIALS

Premature optimization is the root of all evil.
— Donald E. Knuth

A polynomial over F is *absolutely irreducible* if it is irreducible over an algebraic closure of F, and *relatively irreducible* if it is irreducible over F but factors over some extension field of F. We define

$$\begin{aligned} A_{r,n}(F) &= \{f \in P_{r,n}(F) \colon f \text{ is absolutely irreducible}\} \subseteq I_{r,n}(F), \\ E_{r,n}(F) &= I_{r,n}(F) \setminus A_{r,n}(F). \end{aligned} \tag{2.5.1}$$

As before, we restrict ourselves to finite fields and recall that all our polynomials are monic. For a field extension $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ of degree k, we consider the Galois group $G_k = \mathrm{Gal}(\mathbb{F}_{q^k} : \mathbb{F}_q) \cong \mathbb{Z}_k$. It acts on $\mathbb{F}_{q^k}[x]$ coefficientwise and we have the "norm" map

$$\begin{aligned} \varphi_{r,n,k} \colon P_{r,n/k}(\mathbb{F}_{q^k}) &\to P_{r,n}(\mathbb{F}_q), \\ g &\mapsto \prod_{\sigma \in G_k} g^\sigma, \end{aligned}$$

for each k dividing n. Since $(\varphi_{r,n,k}(g))^\tau = \varphi_{r,n,k}(g)$ for any $\tau \in G_k$ and therefore $\varphi_{r,n,k}(g) \in P_{r,n}(\mathbb{F}_q)$, this map is well-defined.

Relatively irreducible polynomials in $P_{r,n}(\mathbb{F}_q)$ are the product of all conjugates of an irreducible polynomial g defined over some extension field $\mathbb{F}_{q^k}$. If g itself is relatively irreducible over $\mathbb{F}_{q^k}$, then there exists an appropriate multiple j of k and $h \in P_{r,n/j}(\mathbb{F}_{q^j})$ with the same image $\varphi_{r,n,k}(g) = \varphi_{r,n,j}(h)$ in $P_{r,n}(\mathbb{F}_q)$ and the property that h is absolutely irreducible. So, every relatively irreducible polynomial is contained in $\varphi_{r,n,k}(A_{r,n/k}(\mathbb{F}_{q^k}))$ for a unique $k > 1$ dividing n. Furthermore, the absolutely irreducible polynomials in $P_{r,n}(\mathbb{F}_q)$ are exactly those in $\varphi_{r,n,1}(A_{r,n}(\mathbb{F}_q))$, and we summarize

$$A_{r,n}(\mathbb{F}_q) = \varphi_{r,n,1}(A_{r,n}(\mathbb{F}_q)), \tag{2.5.2}$$

$$E_{r,n}(\mathbb{F}_q) \subseteq \bigcup_{1<k\mid n} \varphi_{r,n,k}(A_{r,n/k}(\mathbb{F}_{q^k})). \tag{2.5.3}$$

In order to replace the latter by an equality, we let

$$A^+_{r,n/k}(\mathbb{F}_{q^k}) = A_{r,n/k}(\mathbb{F}_{q^k}) \setminus \bigcup_{s\mid k,\, s\neq k} A_{r,n/k}(\mathbb{F}_{q^s}) \tag{2.5.4}$$

be the set of absolutely irreducible polynomials over $\mathbb{F}_{q^k}$ that are not defined over a proper subfield containing $\mathbb{F}_q$, and

$$I_{r,n,k}(\mathbb{F}_q) = \varphi_{r,n,k}(A^+_{r,n/k}(\mathbb{F}_{q^k})).$$

Lemma 2.5.5. *(i) We have the disjoint union*

$$I_{r,n}(\mathbb{F}_q) = \dot{\bigcup_{k\mid n}} I_{r,n,k}(\mathbb{F}_q) \tag{2.5.6}$$

and more precisely

$$A_{r,n}(\mathbb{F}_q) = I_{r,n,1}(\mathbb{F}_q), \tag{2.5.7}$$

$$E_{r,n}(\mathbb{F}_q) = \dot{\bigcup_{1<k\mid n}} I_{r,n,k}(\mathbb{F}_q). \tag{2.5.8}$$

(ii) $$\#I_{r,n,k}(\mathbb{F}_q) = \tfrac{1}{k}\#A^+_{r,n/k}(\mathbb{F}_{q^k}).$$

Proof. (i) Let $g \in A_{r,n/k}(\mathbb{F}_{q^k})$. By definition, g is monic. The k conjugates g^σ, for $\sigma \in G_k$, are pairwise non-associate if and only if the coefficients are not contained in some proper subfield of $\mathbb{F}_{q^k}$. This shows

$$I_{r,n,k}(\mathbb{F}_q) \subseteq I_{r,n}(\mathbb{F}_q). \tag{2.5.9}$$

Let $f \in I_{r,n}(\mathbb{F}_q)$. Then $f = \varphi_{r,n,k}(g)$ for some $g \in A_{r,n/k}(\mathbb{F}_{q^k})$, with k dividing n as observed in (2.5.3). If g has coefficients

from a subfield of $\mathbb{F}_{q^k}$, say $g \in A_{r,n/k}(\mathbb{F}_{q^s})$ for some $s < k$ dividing k, then g^σ equals g for some $\sigma \in G_k \setminus \{\mathrm{id}\}$. Taking the smallest such s and

$$h = \prod_{\tau \in G_s} g^\tau \in I_{r,n,k/s}(\mathbb{F}_q),$$

we have $h^{k/s} = \varphi_{r,n,k}(g)$. Hence $\varphi_{r,n,k}(g)$ is a (k/s)-th power and therefore reducible, in contradiction to the choice of f. This shows that $g \in A^+_{r,n/k}(\mathbb{F}_{q^k})$ and a fortiori

$$I_{r,n}(\mathbb{F}_q) \subseteq \bigcup_{k \mid n} I_{r,n,k}(\mathbb{F}_q).$$

The disjointness follows from the fact that the factorization of $\varphi_{r,n,k}(g)$ for any $g \in A^+_{r,n/k}(\mathbb{F}_{q^k})$ has exactly k irreducible factors over $\mathbb{F}_{q^n}$, and (2.5.6) follows with (2.5.9).

Finally, (2.5.7) and (2.5.8) follow from (2.5.2) and (2.5.1), respectively.

(ii) Let $g, h \in I_{r,n/k}(\mathbb{F}_{q^k})$. Then $\varphi_{r,n,k}(g) = \varphi_{r,n,k}(h)$ if and only if $h = g^\sigma$ for some automorphism $\sigma \in G_k$. Sufficiency is a direct computation and necessity follows from the unique factorization of $\varphi_{r,n,k}(g)$ and $\varphi_{r,n,k}(h)$ over $\mathbb{F}_{q^k}$. Therefore, the size of each fibre of $\varphi_{r,n,k}$ on $A^+_{r,n/k}(\mathbb{F}_{q^k})$ is $\#G_k = k$. □

We omit the parameter r from the notation of the generating functions and their coefficients. The generating function $A^+(\mathbb{F}_{q^k})$ of $\#A^+_{r,n}(\mathbb{F}_{q^k})$ is related to the generating function $A(\mathbb{F}_q)$ of $\#A_{r,n}(\mathbb{F}_q)$ by definition (2.5.4) and we find by inclusion-exclusion

$$A^+(\mathbb{F}_{q^k}) = \sum_{s \mid k} \mu(k/s) A(\mathbb{F}_{q^s}).$$

With (2.5.6) and Lemma 2.5.5 (ii), we relate this to the generating function $I(\mathbb{F}_q)$ of irreducible polynomials as introduced in Section 2.2 and obtain

$$\begin{aligned} [z^n] I(\mathbb{F}_q) &= \sum_{k \mid n} \frac{1}{k} \sum_{s \mid k} \mu(k/s) \cdot [z^{n/k}] A(\mathbb{F}_{q^s}), \\ [z^n] A(\mathbb{F}_q) &= \sum_{k \mid n} \frac{1}{k} \sum_{s \mid k} \mu(s) \cdot [z^{n/k}] I(\mathbb{F}_{q^s}) \end{aligned} \tag{2.5.10}$$

with Möbius inversion.

A Maple program to compute the latter is shown in Figure 2.5.11. Exact values for $\#E_{2,n}(\mathbb{F}_q)$ with $n \leqslant 6$ are given in von zur Gathen (2008, Table 4.1). We extend this in Table 2.5.12.

For an explicit formula, we combine the expression for $I_n(\mathbb{F}_q) = I_n$ from Theorem 2.2.7 with (2.5.10).

n	$\#E_{2,n}(\mathbb{F}_q)$
1	0
2	$(q^4 - q)/2$
3	$(q^6 + q^3 - q^2 - q)/3$
4	$(2\,q^{10} + q^8 - 2\,q^5 - 2\,q^4 + q^2)/4$
5	$(q^{10} + q^5 - q^2 - q)/5$
6	$(3\,q^{18} + 3\,q^{16} + 2\,q^{15} - 2\,q^{12} - 3\,q^{10} - 3\,q^9 - 3\,q^8 + q^6 + q^5 - q^4 - q^3 + 2\,q^2 + q)/6$
7	$(q^{14} + q^7 - q^2 - q)/7$
8	$(4\,q^{28} + 4\,q^{26} + 4\,q^{24} - 6\,q^{20} - 8\,q^{18} - 3\,q^{16} - 4\,q^{13} + 6\,q^{10} + 8\,q^9 + 2\,q^8 - 4\,q^7 - 4\,q^6 + q^4)/8$

n	$\#E_{3,n}(\mathbb{F}_q)$
1	0
2	$(q^6 + q^4 - q^3 - q)/2$
3	$(q^9 + q^6 - q^2 - q)/3$
4	$(2\,q^{18} + 2\,q^{16} + 2\,q^{14} + q^{12} - 2\,q^9 - 3\,q^8 - 2\,q^7 - 3\,q^6 + 2\,q^3 + q^2)/4$
5	$(q^{15} + q^{10} + q^5 - q^3 - q^2 - q)/5$
6	$(3\,q^{38} + 3\,q^{36} + 3\,q^{34} + 3\,q^{32} + 3\,q^{30} + 3\,q^{28} + 2\,q^{27} + 3\,q^{26} + 2\,q^{24} - 3\,q^{22} + 2\,q^{21} - 6\,q^{20} - 3\,q^{19} - 11\,q^{18} - 3\,q^{17} - 9\,q^{16} - 3\,q^{15} - 6\,q^{14} - 3\,q^{13} - q^{12} + 3\,q^{11} + 9\,q^{10} + 4\,q^9 + 7\,q^8 + q^7 - 3\,q^6 - 3\,q^5 - 2\,q^4 + 2\,q^3 + 2\,q^2 + q)/6$
7	$(q^{21} + q^{14} + q^7 - q^3 - q^2 - q)/7$

n	$\#E_{4,n}(\mathbb{F}_q)$
1	0
2	$(q^8 + q^6 - q^3 - q)/2$
3	$(q^{12} + q^9 + q^6 - q^4 - q^2 - q)/3$
4	$(2\,q^{28} + 2\,q^{26} + 2\,q^{24} + 2\,q^{22} + 2\,q^{20} + 2\,q^{18} + q^{16} - 2\,q^{14} - 2\,q^{13} - 3\,q^{12} - 2\,q^{11} - 4\,q^{10} - 2\,q^9 - 4\,q^8 - q^6 + 2\,q^5 + 2\,q^4 + 2\,q^3 + q^2)/4$
5	$(q^{20} + q^{15} + q^{10} + q^5 - q^4 - q^3 - q^2 - q)/5$
6	$(3\,q^{68} + 3\,q^{66} + 3\,q^{64} + 3\,q^{62} + 3\,q^{60} + 3\,q^{58} + 3\,q^{56} + 3\,q^{54} + 3\,q^{52} + 3\,q^{50} + 3\,q^{48} + 3\,q^{46} + 3\,q^{44} + 5\,q^{42} + 3\,q^{40} + 2\,q^{39} + 3\,q^{38} + 2\,q^{36} - 6\,q^{34} - q^{33} - 9\,q^{32} - 3\,q^{31} - 10\,q^{30} - 3\,q^{29} - 15\,q^{28} - q^{27} - 15\,q^{26} - 3\,q^{25} - 14\,q^{24} - 3\,q^{23} - 12\,q^{22} - 3\,q^{21} - 9\,q^{20} - 3\,q^{19} - 4\,q^{18} + 3\,q^{17} + 9\,q^{16} + 7\,q^{15} + 16\,q^{14} + 10\,q^{13} + 12\,q^{12} + 7\,q^{11} + 10\,q^{10} - 2\,q^9 - q^8 - 6\,q^7 - 7\,q^6 - 4\,q^5 + q^4 + 2\,q^3 + 2\,q^2 + q)/6$

Table 2.5.12: Exact values of $\#E_{r,n}(\mathbb{F}_q)$ for small values of r and n.

```
absirreds:=proc(n,r) local k,s: option remember:
    add(1/k*add(mobius(s)*subs(q=q^s,coeff(irreduciblesGF(
        z,n/k,r),z^(n/k))),s=divisors(k)),k=divisors(n))
end:

absirredsGF:=proc(z,N,r) local k,s: option remember:
    sum('absirreds(k,r)*z^k',k=1..N)
end:

relirredsGF:=proc(z,N,r) option remember:
    irreduciblesGF(z,N,r)-absirredsGF(z,N,r);
end:

relirreds:=proc(n,r)
    coeff(sort(expand(relirredsGF(z,n,r))),z^n):
end:
```

Figure 2.5.11: Maple program to compute the number of relatively irreducible polynomials in r variables of degree n.

Theorem 2.5.13. *For* $r, n \geqslant 1$, $q \geqslant 2$, M_n *as in* (2.2.6), *and* $P_n(\mathbb{F}_q) = P_n$ *as in* (2.2.1), *we have*

$$\begin{aligned}
A_0(\mathbb{F}_q) &= 0,\\
A_n(\mathbb{F}_q) &= -\sum_{s\,|\,k\,|\,n} \frac{\mu(s)}{k} \sum_{m\,|\,n/k} \frac{\mu(m)}{m}\\
&\qquad \sum_{j\in M_{n/(km)}} \frac{(-1)^{|j|}}{|j|} P_{j_1}(\mathbb{F}_{q^s}) P_{j_2}(\mathbb{F}_{q^s}) \cdots P_{j_{|j|}}(\mathbb{F}_{q^s}),\\
E_0(\mathbb{F}_q) &= 0,\\
E_n(\mathbb{F}_q) &= -\sum_{1<k\,|\,n} \frac{1}{k} \sum_{s\,|\,k} \mu(s) I_{n/k}(\mathbb{F}_{q^s}) \qquad (2.5.14)\\
&= \sum_{1<k\,|\,n} \frac{1}{k} \sum_{\substack{s\,|\,k\\ m\,|\,n/k}} \frac{\mu(s)\mu(m)}{m}\\
&\qquad \cdot \sum_{j\in M_{n/(km)}} \frac{(-1)^{|j|}}{|j|} P_{j_1}(\mathbb{F}_{q^s}) P_{j_2}(\mathbb{F}_{q^s}) \cdots P_{j_{|j|}}(\mathbb{F}_{q^s}).
\end{aligned}$$

We check that for $r = 1$ we obtain the expected result

$$A_n(\mathbb{F}_q) = \begin{cases} q & \text{if } n = 1,\\ 0 & \text{if } n > 1. \end{cases}$$

To this end, we use the well-known fact that

$$\sum_{s\,|\,n}\mu(s)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{if } n>1.\end{cases}$$

From (2.5.15) and (2.2.8) we have

$$\begin{aligned}nA_n(\mathbb{F}_q)&=\sum_{\substack{s\,|\,k\,|\,n\\ t\,|\,n/k}}\mu(s)\mu(t)q^{\frac{ns}{kt}}=\sum_{\substack{s\,|\,k\,|\,n\\ a\,|\,n/k}}\mu(s)\mu(n/(ka))q^{sa}\\ &=\sum_{m\,|\,n}q^m\sum_{\substack{s\,|\,k\,|\,n\\ m=sa,\,a\,|\,n/k}}\mu(s)\mu(n/(ka))=\sum_{m\,|\,n}q^m\sum_{s\,|\,m}\mu(s)\sum_{\substack{s\,|\,k\,|\,n\\ m/s\,|\,n/k}}\mu(ns/(mk))\\ &=\sum_{m\,|\,n}q^m\sum_{s\,|\,m}\mu(s)\sum_{j\,|\,n/m}\mu(n/(mj))\\ &=\sum_{m\,|\,n}q^m\sum_{s\,|\,m}\mu(s)\sum_{i\,|\,n/m}\mu(i)=\begin{cases}q & \text{if } n=1,\\ 0 & \text{if } n>1,\end{cases}\end{aligned}$$

where $a=n/(kt)$, $m=as$, $j=k/s$, and $i=n/(mj)$.

The remainder of this section deals with the case $r\geqslant 2$. For the approach by symbolic generating functions, we define, with $I(\mathbf{q},z)$ as in (2.2.12), the two power series $A,E\in\mathbb{Q}(\mathbf{q})[\![z]\!]$ by

$$\begin{aligned}A_0(\mathbf{q})&=I_0(\mathbf{q})=0,\\ A_n(\mathbf{q})&=\sum_{k\,|\,n}\frac{1}{k}\sum_{s\,|\,k}\mu(s)I_{n/k}(\mathbf{q}^s)\in\mathbb{Z}[\mathbf{q}]\text{ for }n>0, \qquad (2.5.15)\\ A(\mathbf{q},z)&=\sum_{n\geqslant 0}A_n(\mathbf{q})z^n\in\mathbb{Z}[\mathbf{q}][\![z]\!],\\ E(\mathbf{q},z)&=I(\mathbf{q},z)-A(\mathbf{q},z)\\ &=-\sum_{1<k\,|\,n}\frac{1}{k}\sum_{s\,|\,k}\mu(s)I_{n/k}(\mathbf{q}^s)\in\mathbb{Z}[\mathbf{q}][\![z]\!]. \qquad (2.5.16)\end{aligned}$$

Then

$$\begin{aligned}A_n(q)&=\#A_{r,n}(\mathbb{F}_q),\\ E_n(q)&=\#E_{r,n}(\mathbb{F}_q).\end{aligned}$$

The inner sum of (2.5.16) has degree $\deg_{\mathbf{q}}I_{n/k}(\mathbf{q}^k)$ in $\mathbf{q}$. Let n be composite and ℓ its smallest prime divisor. For $k=\ell$, this inner sum consists of only two terms and we find

$$\begin{aligned}E_n(\mathbf{q})&=\frac{1}{\ell}(I_{n/\ell}(\mathbf{q}^\ell)-I_{n/\ell}(\mathbf{q}))-\sum_{\ell<k\,|\,n}\frac{1}{k}\sum_{s|k}\mu(s)I_{n/k}(\mathbf{q}^s)\\ &=\frac{1}{\ell}(P_{n/\ell}(\mathbf{q}^\ell)-R_{n/\ell}(\mathbf{q}^\ell)-I_{n/\ell}(\mathbf{q}))+O(\mathbf{q}^{\max_{\ell<k|n}w_{r,n}(k)}),\end{aligned} \qquad (2.5.17)$$

summand	$\deg_{\mathbf{q}}$
$P_{n/\ell}(\mathbf{q}^\ell)$	$\ell(b_{r,n/\ell} - 1) = w_{r,n}(\ell)$
$R_{n/\ell}(\mathbf{q}^\ell)$	$\ell(b_{r,n/\ell-1} + r - 1) = w_{r,n}(\ell) - \ell(b_{r-1,n/\ell} - r)$
$I_{n/\ell}(\mathbf{q})$	$b_{r,n/\ell} - 1 = \frac{1}{\ell} w_{r,n}(\ell)$
$\sum_{\ell<k\mid n} I_{n/k}(\mathbf{q}^k)$	$\leqslant \max_{\ell<k\mid n} w_{r,n}(k)$

Table 2.5.19: Summands of E and their degrees in $\mathbf{q}$.

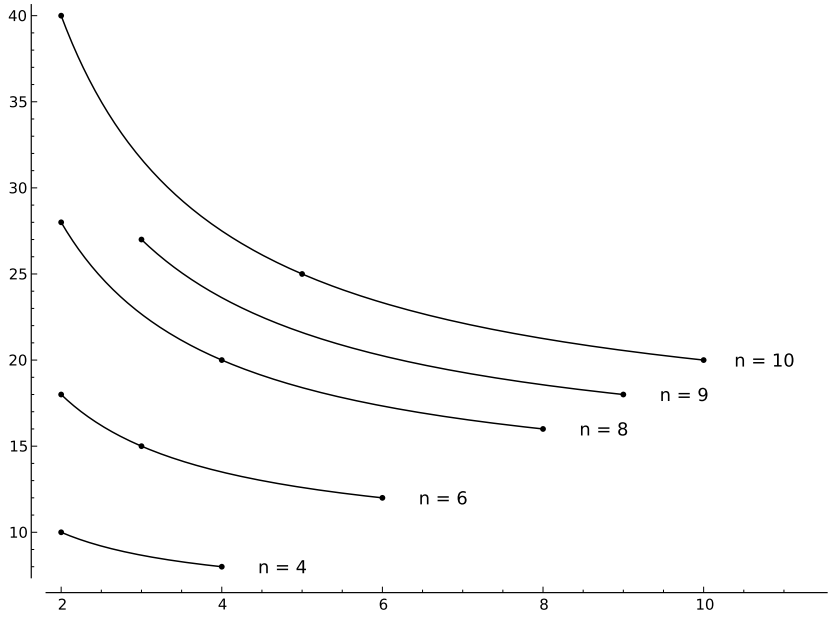

Figure 2.5.20: Graphs for $w_{2,n}(k)$ on $[\ell, n]$ for composite n in the range from 4 to 10, where ℓ denotes the smallest prime divisor of n. The dots represent the values at divisors of n.

with

$$w_{r,n}(k) = \deg_{\mathbf{q}}(I_{n/k}(\mathbf{q}^k)) = \deg_{\mathbf{q}}(P_{n/k}(\mathbf{q}^k)) = k((r + n/k)^{\underline{r}}/r! - 1) \tag{2.5.18}$$

for any divisor k of n. Table 2.5.19 lists the degree in $\mathbf{q}$ for all summands in (2.5.17). We consider $w_{r,n}$ as a function on the real interval $[1, n]$, see Figure 2.5.20.

Lemma 2.5.21. *Let $r \geqslant 2$, n be composite, ℓ the smallest and k_2 the second smallest divisor of n greater than 1.*

(i) The function $w_{r,n}(k)$ is strictly decreasing in k on $[1, n]$.

(ii) For composite $n \neq 4, 6$, we have

$$w_{r,n}(\ell) - w_{r,n}(k_2) - w_{r-1,n}(\ell) \geqslant 0. \tag{2.5.22}$$

(iii) For composite $n > \ell k_2$ *different from* 12*, we have*

$$w_{r,n}(\ell) - w_{r,n}(k_2) - w_{r-1,n}(\ell) \geqslant \log_2 n - 2. \tag{2.5.23}$$

This also holds if $n = 12$ *and* $r \geqslant 3$.

The inequality (2.5.22) is false when n is 4 or 6, and (2.5.23) is false for $n = 12$, $r = 2$.

Proof. (i) We compute

$$\begin{aligned} w'_{r,n}(k) &= \frac{(r+n/k)^{\underline{r}}}{r!} - \frac{n}{r!k} \sum_{1 \leqslant i \leqslant r} \frac{(r+n/k)^{\underline{r}}}{i+n/k} - 1 \\ &= \frac{(r+n/k)^{\underline{r}}}{r!}\Big(1 - \sum_{1 \leqslant i \leqslant r} \frac{1}{1+i\frac{k}{n}}\Big) - 1. \end{aligned} \tag{2.5.24}$$

If $r \geqslant 3$, then

$$\sum_{1 \leqslant i \leqslant r} \frac{1}{1+i\frac{k}{n}} \geqslant \sum_{1 \leqslant i \leqslant 3} \frac{1}{1+i} > 1$$

for all $1 \leqslant k \leqslant n$, which proves $w'_{r,n}(k) < 0$.

If $r = 2$, we evaluate (2.5.24) as

$$w'_{2,n}(k) = \frac{(1+n/k)(2+n/k)}{2}\Big(1 - \frac{1}{1+k/n} - \frac{1}{1+2k/n}\Big) - 1 = -\frac{n^2}{2k^2}$$

to find $w'_{2,n}(k) < 0$ for all k.

For (ii) and (iii), we first show that the sequence $a_{r,n} = w_{r,n}(\ell) - w_{r-1,n}(\ell) - w_{r,n}(k_2) = \ell b_{r,n/l-1} - k_2(b_{r,n/k_2} - 1)$ is monotonically increasing in r. We have

$$a_{r,n} - a_{r-1,n} = \ell b_{r,n/\ell-2} - k_2 b_{r,n/k_2-1} \geqslant 0$$

if and only if

$$A_{r,n} = \frac{\ell(r+n/\ell-2)^{\underline{r}}}{k_2(r+n/k_2-1)^{\underline{r}}} \geqslant 1$$

and prove the latter by induction on $r \geqslant 2$.

For $r = 2$, we have to prove

$$n(k_2 - \ell) \geqslant 2\ell k_2. \tag{2.5.25}$$

If $k_2 = \ell + 1$, then $\ell = 2$, $k_2 = 3$ and since we exclude $n = 6$, we have $n \geqslant 12$ to show (2.5.25). If $k_2 \geqslant \ell + 2$, we distinguish two cases. Now, $k_2 = n$ if and only if $n = \ell^2$. Since we exclude $n = 4$, we then have $\ell \geqslant 3$ and (2.5.25) follows. If $k_2 \neq n$, then $k_2 \leqslant \sqrt{n} < n$ and therefore $2\ell k_2 < 2\sqrt{n}\sqrt{n} \leqslant (k_2 - \ell)n$.

For the induction step, we have

$$A_{r,n} = A_{r-1,n}\frac{n/\ell - 2 + r}{n/k_2 - 1 + r} \geqslant \frac{n/\ell - 2 + r}{n/k_2 - 1 + r} \geqslant 1,$$

where the last inequality is equivalent to $n(k_2 - \ell) \geqslant \ell k_2$, which follows from (2.5.25).

With this monotonicity of $a_{r,n}$ in r, it is sufficient to check (ii) and (iii) for the smallest admissible value of r.

(ii) We have

$$a_{2,n} = \frac{n}{2}\Big(\frac{n}{\ell} - \frac{n}{k_2} - 2\Big). \tag{2.5.26}$$

For

- $n = \ell^2$, $\ell \neq 4$,
- $n = \ell k_2$, $n \neq 6$, or
- $n = 12$,

this is non-negative by direct computation, and in the remaining case, $n > \ell k_2$ different from 12, by (iii).

(iii) For $n > \ell k_2$ different from 12, we have $n/\ell - n/k_2 \geqslant 3$ and find with (2.5.26)

$$a_{2,n} \geqslant \frac{n}{2} > \log_2 n - 2.$$

For $n = 12$ and $r \geqslant 3$, we compute directly $a_{3,12} = 10 > \log_2 12 - 2$. □

This lemma allows us to order the summands in (2.5.17) by $\deg_{\mathbf{q}}$, and the approach by generating functions gives the following result.

Theorem 2.5.27. *Let $r, n \geqslant 2$, let ℓ be the smallest prime divisor of n, and*

$$\epsilon_{r,n}(\mathbf{q}) = \frac{\mathbf{q}^{\ell\left(\binom{r+n/\ell}{r}-1\right)}}{\ell(1-\mathbf{q}^{-\ell})} \in \mathbb{Q}(\mathbf{q}),$$
$$\kappa = (\ell-1)\Big(\binom{r-1+n/\ell}{r-1} - r\Big) + 1.$$

Then the following hold.

(i) $\mathsf{E}_1(\mathbf{q}) = 0$.

(ii) If n is prime, then

$$\mathsf{E}_n(\mathbf{q}) = \epsilon_{r,n}(\mathbf{q})(1-\mathbf{q}^{-nr})\Big(1 - \mathbf{q}^{-r(n-1)}\frac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-n})}{(1-\mathbf{q}^{-1})(1-\mathbf{q}^{-nr})}\Big).$$

(iii) If n is composite, then $\kappa \geqslant 2$ and

$$\mathsf{E}_n(\mathbf{q}) = \epsilon_{r,n}(\mathbf{q})(1 + O(\mathbf{q}^{-\kappa})).$$

Proof. For $n = 1$, the sum (2.5.14) is empty and this shows (i). For $n = \ell$ prime, (2.5.14) simplifies to $E_n(\mathbf{q}) = (I_1(\mathbf{q}^\ell) - I_1(\mathbf{q}))/\ell = (P_1(\mathbf{q}^\ell) - P_1(\mathbf{q}))/\ell$, since $I_1 = P_1$ by Theorem 2.2.16 and (ii) follows.

For composite n, the product $(\ell-1)(b_{r-1,n/\ell} - r)$ is positive and therefore $\kappa \geqslant 2$. We recall the summands of (2.5.17) in Table 2.5.19. Lemma 2.5.21 (i) shows that $\max_{\ell<k\mid n} w_{r,n}(k) = w_{r,n}(k_2)$ and we find

$$E_n(\mathbf{q}) = \frac{1}{\ell}(P_{n/\ell}(\mathbf{q}^\ell) - R_{n/\ell}(\mathbf{q}^\ell) - I_{n/\ell}(\mathbf{q})) + O(\mathbf{q}^{w_{r,n}(k_2)}).$$

Since $b_{r-1,n/\ell} - r > 0$ for composite n, we identify with Lemma 2.5.21 (i) as main term $P_{n/\ell}(\mathbf{q}^\ell)/\ell = \epsilon_{r,n}(\mathbf{q})(1-\mathbf{q}^{-\ell b_{r-1,n/\ell}})$. For the summands of

$$E_n(\mathbf{q})/\epsilon_{r,n}(\mathbf{q}) = (1-\mathbf{q}^{-\ell b_{r-1,n/\ell}})\Big(1 - \frac{R_{n/\ell}(\mathbf{q}^\ell)}{P_{n/\ell}(\mathbf{q}^\ell)} - \frac{I_{n/\ell}(\mathbf{q})}{P_{n/\ell}(\mathbf{q}^\ell)}\Big) + O(\mathbf{q}^{w_{r,n}(k_2) - \deg_{\mathbf{q}} P_{n/\ell}(\mathbf{q}^\ell)})$$

we find as degrees in $\mathbf{q}$

$$\begin{aligned} -\ell b_{r-1,n/\ell} &\leqslant -\kappa, \\ \deg_{\mathbf{q}} R_{n/\ell}(\mathbf{q}^\ell) - \deg_{\mathbf{q}} P_{n/\ell}(\mathbf{q}^\ell) &= -\ell(b_{r-1,n/\ell} - r) \leqslant -\kappa, \quad (2.5.28) \\ \deg_{\mathbf{q}} I_{n/\ell}(\mathbf{q}) - \deg_{\mathbf{q}} P_{n/\ell}(\mathbf{q}^\ell) &= -(\ell-1)(b_{r,n/\ell} - 1) \leqslant -\kappa, \quad (2.5.29) \\ w_{r,n}(k_2) - \deg_{\mathbf{q}} P_{n/\ell}(\mathbf{q}^\ell) &\leqslant -\ell(b_{r-1,n/\ell} - 1) \leqslant -\kappa \quad (2.5.30) \end{aligned}$$

for $n \neq 4, 6$ by Lemma 2.5.21 (ii). When n is 4 or 6, the last inequality in (2.5.30) is false, but still

$$w_{r,n}(k_2) - \deg_{\mathbf{q}} P_{n/\ell}(\mathbf{q}^\ell) \leqslant -\kappa. \quad \square \qquad (2.5.31)$$

On closer inspection, it is possible to partition for each composite n the range for r into two non-empty intervals, where either the difference in (2.5.28) or the difference in (2.5.29) dominates all others. This provides tighter bounds at the cost of further case distinctions.

The combinatorial approach yields the following result.

Theorem 2.5.32. *Let $r, q \geqslant 2$, and $\epsilon_{r,n}$ and κ as in Theorem 2.5.27.*

(i) $\#E_{r,1}(\mathbb{F}_q) = 0$.

(ii) If n is prime, then

$$\#E_{r,n}(\mathbb{F}_q) = \epsilon_{r,n}(q)(1-q^{-nr})\Big(1 - q^{-r(n-1)}\frac{(1-q^{-r})(1-q^{-n})}{(1-q^{-1})(1-q^{-nr})}\Big), \qquad (2.5.33)$$

$$0 \leqslant \epsilon_{r,n}(q) - \#E_{r,n}(\mathbb{F}_q) \leqslant 3q^{-r(n-1)}.$$

(iii) If n is composite, then

$$|\#E_{r,n}(\mathbb{F}_q) - \epsilon_{r,n}(q)| \leqslant \epsilon_{r,n}(q) \cdot 3q^{-\kappa}.$$

Proof. The exact statements of (i) and (ii) were already shown in Theorem 2.5.27 and in (2.5.33) we have $q^{-r(n-1)}/16$ as upper bound for q^{-nr} and $32q^{-r(n-1)}/15$ as upper bound for the last subtracted term.

For (iii), let ℓ be the smallest and k_2 the second smallest divisor of n greater than 1. We prove that

$$\#E_{r,n}(\mathbb{F}_q) \geqslant \epsilon_{r,n}(q)(1-3q^{-\kappa}), \tag{2.5.34}$$

$$\#E_{r,n}(\mathbb{F}_q) \leqslant \epsilon_{r,n}(q)(1+2q^{-\ell(b_{r-1,n/\ell}-1)}) \quad \text{for } n \neq 4,6, \tag{2.5.35}$$

$$\#E_{r,n}(\mathbb{F}_q) \leqslant \epsilon_{r,n}(q)(1+q^{-\kappa}) \quad \text{for } n = 4,6. \tag{2.5.36}$$

We begin with (2.5.34) and have from Lemma 2.5.5 (ii)

$$\begin{aligned}\#E_{r,n}(\mathbb{F}_q) &\geqslant \#I_{r,n,\ell}(\mathbb{F}_q) = \frac{1}{\ell}\#A^+_{r,n/\ell}(\mathbb{F}_{q^\ell}) \\ &= \frac{1}{\ell}(\#I_{r,n/\ell}(\mathbb{F}_{q^\ell}) - \#I_{r,n/\ell}(\mathbb{F}_q)),\end{aligned}$$

since ℓ is prime and there are no proper intermediate fields between $\mathbb{F}_q$ and $\mathbb{F}_{q^\ell}$. With the lower bound on the number of irreducible polynomials from Corollary 2.3.14 this yields

$$\begin{aligned}\#E_{r,n}(\mathbb{F}_q) &\geqslant \frac{1}{\ell}(\#P_{r,n/\ell}(\mathbb{F}_{q^\ell}) - 2\rho_{r,n/\ell}(q^\ell) - \#P_{r,n/\ell}(\mathbb{F}_q)) \\ &= \epsilon_{r,n}(q)\Big(1 - q^{-\ell b_{r-1,n/\ell}} - 2q^{-\ell(b_{r-1,n/\ell}-r)}\frac{1-q^{-\ell r}}{1-q^{-\ell}} \\ &\quad - q^{-(\ell-1)(b_{r,n/\ell}-1)}\frac{(1-q^{-b_{r-1,n/\ell}})(1-q^{-\ell})}{1-q^{-1}}\Big) \\ &= \epsilon_{r,n}(q)\Big(1-q^{-\kappa}\Big(q^{-b_{r-1,n/\ell}-\ell r+1} + 2q^{-b_{r-1,n/\ell}+r+1}\frac{1-q^{-\ell r}}{1-q^{-\ell}} \\ &\quad + q^{-(\ell-1)b_{r,n/\ell-1}-\ell r+\ell+r}\frac{(1-q^{-b_{r-1,n/\ell}})(1-q^{-\ell})}{1-q^{-1}}\Big)\Big) \\ &\geqslant \epsilon_{r,n}(q)(1-q^{-\kappa}(1/16+8/3+1/4)) \\ &\geqslant \epsilon_{r,n}(q)(1-3q^{-\kappa}).\end{aligned}$$

For the lower bounds (2.5.35) and (2.5.36), we have from Lemma 2.5.5 (ii)

$$\begin{aligned}\#I_{r,n,k}(\mathbb{F}_q) &= \frac{1}{k}\#A^+_{r,n/k}(\mathbb{F}_{q^k}) \\ &\leqslant \frac{1}{k}\#P_{r,n/k}(\mathbb{F}_{q^k}) \\ &= q^{w_{r,n}(k)}\frac{1-q^{-k\binom{n/k+r-1}{r-1}}}{k(1-q^{-k})},\end{aligned}$$

with $w_{r,n}(k)$ as defined in (2.5.18). We obtain with (2.5.8)

$$\#E_{r,n}(\mathbb{F}_q) \leqslant \sum_{1<k|n} \#I_{r,n,k}(\mathbb{F}_q)$$

$$\begin{aligned}
&\leqslant \sum_{1<k\mid n} q^{w_{r,n}(k)} \cdot \frac{1-q^{-kb_{r-1,n/k}}}{k(1-q^{-k})} \\
&= q^{w_{r,n}(\ell)} \frac{1-q^{-\ell b_{r-1,n/\ell}}}{\ell(1-q^{-\ell})} + \sum_{\ell<k\mid n} q^{w_{r,n}(k)} \frac{1-q^{-kb_{r-1,n/k}}}{k(1-q^{-k})} \\
&= \epsilon_{r,n}(q)(1-q^{-\ell b_{r-1,n/\ell}}) \\
&\quad \cdot \Big(1 + q^{-w_{r,n}(\ell)} \sum_{\ell<k\mid n} q^{w_{r,n}(k)} \frac{\ell(1-q^{-\ell})(1-q^{-kb_{r-1,n/k}})}{k(1-q^{-k})(1-q^{-\ell b_{r-1,n/\ell}})}\Big) \\
&\leqslant \epsilon_{r,n}(q)\Big(1 + q^{-w_{r,n}(\ell)} \sum_{\ell<k\mid n} \frac{\ell}{k} q^{w_{r,n}(k)}\Big), \qquad (2.5.37)
\end{aligned}$$

since $(1-q^{-k})/(1-q^{-kb_{r-1,n/k}})$ is monotone increasing with k.

For $n = \ell^2$ or $n = \ell k_2$, we compute directly from (2.5.37)

$$\begin{aligned}
\#E_{r,\ell^2}(\mathbb{F}_q) &\leqslant \epsilon_{r,n}(q)\Big(1 + \frac{1}{\ell} q^{-w_{r,n}(\ell)+w_{r,n}(n)}\Big), \\
\#E_{r,\ell k_2}(\mathbb{F}_q) &\leqslant \epsilon_{r,n}(q)\Big(1 + q^{-w_{r,n}(\ell)+w_{r,n}(k_2)}\Big(\frac{\ell}{k_2} + \frac{\ell}{n}\Big)\Big) \\
&\leqslant \epsilon_{r,n}(q)(1 + q^{-w_{r,n}(\ell)+w_{r,n}(k_2)}),
\end{aligned}$$

respectively. These prove (2.5.35) for $n \neq 4, 6$, since $-w_{r,n}(\ell) + w_{r,n}(k_2) \leqslant -w_{r-1,n}(\ell) \leqslant -\kappa$ by Lemma 2.5.21 (ii), and they also show (2.5.36) for $n = 4, 6$ with (2.5.31).

For $n > \ell k_2$, we show

$$q^{-w_{r,n}(\ell)} \sum_{\ell<k\mid n} \frac{\ell}{k} q^{w_{r,n}(k)} \leqslant 2q^{-w_{r-1,n}(\ell)}. \qquad (2.5.38)$$

We use the coarse bound $\#\{k\colon \ell < k \mid n\} \leqslant n/2 = 2^{\log_2 n - 1} \leqslant 2q^{\log_2 n - 2}$ and show the stronger

$$q^{-w_{r,n}(\ell)} 2q^{\log_2 n - 2} q^{w_{r,n}(k_2)} \leqslant 2q^{-w_{r-1,n}(\ell)}$$

or equivalently

$$-w_{r,n}(\ell) + w_{r,n}(k_2) \leqslant -w_{r-1,n}(\ell) - \log_2 n + 2.$$

For $n \neq 12$ or $n = 12$ and $r \geqslant 3$, this follows from Lemma 2.5.21 (iii). For $r = 2$ and $n = 12$, it suffices to evaluate left- and right-hand side of (2.5.38) to find $5/6q^{-12} < 2q^{-12}$ as claimed.

Finally, we combine the bounds (2.5.34), (2.5.35), and (2.5.36) with $-w_{r-1,n}(\ell) \leqslant -\kappa$ from (2.5.30). □

Figure 2.5.39 shows plots of $(E_{r,n}(\mathbf{q}) - \epsilon_{r,n}(\mathbf{q}))/(\epsilon_{r,n}(\mathbf{q})\mathbf{q}^{-\kappa})$ for $r = 2$ and $n = 4, 6, 8, 9$, as we substitute for $\mathbf{q}$ real numbers from 2 to 10.

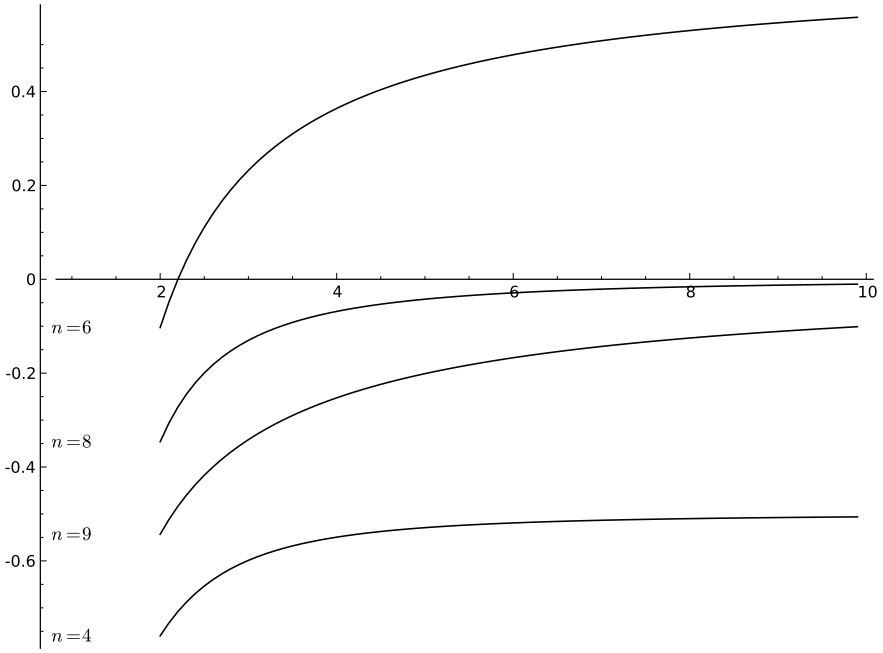

Figure 2.5.39: The normalized relative error in Theorem 2.5.27 (iii) for $r = 2$.

Remark 2.5.40. The bivariate result of von zur Gathen (2008) approximates the ratio $\#E_{2,n}(\mathbb{F}_q)/\#P_{2,n}(\mathbb{F}_q)$ by

$$\frac{q^{-n^2(\ell-1)/(2\ell)}(1-q^{-1})}{\ell(1-q^{-\ell})(1-q^{-n-1})}.$$

This differs from the approximation by $\epsilon_{2,n}(q)/\#P_{2,n}(\mathbb{F}_q)$ in Theorem 2.5.32 by a factor of $1-q^{-n-1}$.

We append some handy bounds.

Corollary 2.5.41. *Let $r, n, q \geqslant 2$, and ℓ be the smallest prime divisor of n, then*

$$\frac{1}{4\ell}q^{\ell\binom{r+n/\ell}{r}-\ell} \leqslant \#E_{r,n}(\mathbb{F}_q) \leqslant \frac{2}{\ell}q^{\ell\binom{1+n/\ell}{r}-\ell},$$

$$\frac{1}{8\ell}q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1} \leqslant \frac{\#E_{r,n}(\mathbb{F}_q)}{\#P_{r,n}(\mathbb{F}_q)} \leqslant \frac{2}{\ell}q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1},$$

$$\frac{1}{8\ell}q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1} \leqslant \frac{\#E_{r,n}(\mathbb{F}_q)}{\#I_{r,n}(\mathbb{F}_q)} \leqslant \frac{2}{\ell}q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1}.$$

The last inequalities follow with Corollary 2.3.13 for $n \geqslant 5$ and by computation with the exact expressions otherwise. We conclude with bounds for the number of absolutely irreducible polynomials by combining Corollary 2.3.14 and Theorem 2.5.32.

Corollary 2.5.42. *Let $r, n, q \geqslant 2$, and $\rho_{r,n}(q)$ as in* (2.2.17)*. Then*

$$\#P_{r,n}(\mathbb{F}_q) - 4\rho_{r,n}(q) \leqslant \#A_{r,n}(\mathbb{F}_q) \leqslant \#I_{r,n}(\mathbb{F}_q) \leqslant \#P_{r,n}(\mathbb{F}_q),$$

where the 4 can be replaced by 3 for $n \geqslant 3$.

2.6 CONCLUSION AND FUTURE WORK

> Civilization advances by extending the number of
> important operations which we can perform
> without thinking about them.
> — Alfred North Whitehead

We have provided exact formulas for the numbers of reducible (Sections 2.2–2.3), s-powerful (Section 2.4), and relatively irreducible polynomials (Section 2.5). The latter also yielded the number of absolutely reducible polynomials.

Further types of multivariate polynomials that are examined from a counting perspective include singular bivariate ones (von zur Gathen, 2008) and pairs of coprime polynomials (Hou & Mullen, 2009). It remains open to extend the methods of this chapter to singular multivariate ones and achieve exponentially decreasing error bounds for coprime multivariate polynomials.

Part II

DECOMPOSABLE POLYNOMIALS

Science is knowledge which we understand so well that we can teach it to a computer; and if we don't fully understand something, it is an art to deal with it. [...] We should continually be striving to transform every art into a science: in the process, we advance the art.
— Donald E. Knuth

All is fair in war, love, and mathematics.
— Eric Temple Bell

> You probably think that one knows everything about polynomials. Most mathematicians would think that, including myself.
> — Serge Lang

The *composition* of two univariate polynomials $g, h \in F[x]$ over a field F is denoted as $f = g \circ h = g(h)$, and then (g, h) is a *decomposition* of f, and f is *decomposable* if g and h have degree at least 2. In the 1920s, Ritt, Fatou, and Julia studied structural properties of these decompositions over $\mathbb{C}$, using analytic methods. Particularly important are two theorems by Ritt on the uniqueness, in a suitable sense, of decompositions, the first one for (many) indecomposable components and the second one for two components, as above. Engstrom (1941) and Levi (1942) proved them over arbitrary fields of characteristic zero using algebraic methods.

The theory was extended to arbitrary characteristic by Fried & MacRae (1969), Dorey & Whaples (1974), Schinzel (1982, 2000), Zannier (1993), and others. Its use in a cryptographic context was suggested by Cade (1985). In computer algebra, the decomposition method of Barton & Zippel (1985) requires exponential time. A fundamental dichotomy is between the *tame case*, where the characteristic p of F does not divide $\deg g$, and the *wild case*, where p divides $\deg g$, see von zur Gathen (1990a,b). (Schinzel (2000, § 1.5) uses *tame* in a different sense.) A breakthrough result of Kozen & Landau (1989) was their polynomial-time algorithm to compute tame decompositions; see also von zur Gathen, Kozen & Landau (1987), Kozen, Landau & Zippel (1996), Gutierrez & Sevilla (2006b), and the survey articles of von zur Gathen (2002) and Gutierrez & Kozen (2003) with further references.

In the tame case, Schur's conjecture, as proven by Turnwald (1995), offers a natural connection with the multivariate polynomials of Chapter 2. In this situation, f is indecomposable if $(f(x) - f(y))/(x - y)$ is absolutely irreducible. Aside from natural exceptions, the converse is also true.

In the wild case, considerably less is known, both mathematically and computationally. Zippel (1991) suggests that the block decompositions of Landau & Miller (1985) for determining subfields of algebraic number fields can be applied to decomposing rational functions even in the wild case. A version of Zippel's algorithm by Blankertz (2014) computes in polynomial time all decompositions of a polynomial that are minimal in a certain sense.

It is intuitively clear that the univariate decomposable polynomials form only a small minority among all univariate polynomials over a field. There is an obvious inclusion-exclusion formula for counting. The main issue is then to determine, under a suitable normalization, the number of *collisions*, where essentially different components (g, h) yield the same f. The number of decomposable polynomials of degree

n is thus the number of all pairs (g, h) with $\deg g \cdot \deg h = n$ reduced by the ambiguities introduced by collisions. An important tool for estimating the number of collisions is Ritt's Second Theorem. The first algebraic versions of Ritt's Second Theorem in positive characteristic p required $p > \deg(g \circ h)$. Zannier (1993) reduced this to the milder and more natural requirement $g' \neq 0$ for all g in the collision. His proof works over an algebraically closed field, and Schinzel's (2000) monograph adapts it to finite fields. Von zur Gathen (2014b) gives a normal form with an explicit description of the (non)uniqueness of the parameters.

The task of counting compositions over a finite field of characteristic p was first considered by Giesbrecht (1988). He showed that the decomposable polynomials form an exponentially small fraction of all univariate polynomials. Von zur Gathen (2014a) presents general approximations to the number of decomposable polynomials. These come with satisfactory (rapidly decreasing) relative error bounds except when p divides $n = \deg f$ exactly twice.

Zannier (2007, 2008, 2009) studies a different but related question, namely decompositions $f = g \circ h$ in $\mathbb{C}[x]$ of *sparse* (or *lacunary*) polynomials f, where the number t of terms is fixed, while the corresponding degrees and coefficients may vary. He shows that the sparsity of f implies the sparsity of h, proving a conjecture by Schinzel, and also gives a parametrization of all such f, g, h in terms of varieties (for the coefficients) and lattices (for the exponents). Fuchs & Pethő (2011) and Fuchs & Zannier (2012) follow up with complete descriptions of sparse decomposable rational functions.

In Chapter 3, we classify all collisions of compositions given by a set of degree sequences via a generalization of Ritt's theorems. This gives an exact formula for the number of decomposable polynomials of degree n over a finite field of characteristic coprime to n.

In Chapter 4, we classify all collisions at degree p^2. This determines exactly the number of decomposable polynomials in one of the open wild cases.

3

COUNTING DECOMPOSABLE POLYNOMIALS: THE TAME CASE

> Algebraists like algorithms. Algebra began as a search for algorithms for solving equations, and algebra has never lost its taste for finding recipes for solving classes of problems.
> — Al Cuoco, E. Paul Goldenberg, June Mark

An extended abstract of this chapter will appear in the Proceedings of ISSAC '14, see Section 1.3 for the complete publication history.

Ritt's First Theorem relates complete decompositions of a given polynomial, where all components are indecomposable. Zieve & Müller (2008) turn it into an applicable method and Medvedev & Scanlon (2014) combine this approach with results from model theory to describe the subvarieties of the k-dimensional affine space that are preserved by a coordinatewise polynomial map. Both works lead to slightly different canonical forms for the complete decomposition of a given polynomial. Zieve & Müller (2008) study sequences of *Ritt moves*, where adjacent indecomposable g, h in a complete decomposition are replaced by g^*, h^* with the same composition, but $\deg g = \deg h^* \neq \deg h = \deg g^*$. Such collisions are the theme of Ritt's Second Theorem and von zur Gathen (2014b) presents a normal form with an exact description of the (non)uniqueness of the parameters under Zannier's assumption $g'(g^*)' \neq 0$.

This chapter combines the above "normalizations" of Ritt's theorems in the tame case to classify collisions of two or more decompositions, not necessarily complete and of arbitrary length (Theorems 3.4.2 and 3.4.5). This yields a fast algorithm for the number of decomposable polynomials of degree n over a finite field of characteristic coprime to n (Theorem 3.4.9 and Algorithm 3.4.10).

We proceed as follows. In Sections 3.1–3.2, we fix some notation and establish basic relations. In Section 3.3, we introduce the *relation graph* of a set of collisions which captures the necessary order and possible Ritt moves for any decomposition. In Section 3.4, this information leads to a complete classification of collisions by Theorems 3.4.2 and 3.4.5. We derive a formula for the number of such collisions over a finite field (Theorem 3.4.9) and obtain a fast algorithm

for the number of decomposable polynomials of degree n over a finite field of characteristic coprime to n (Algorithm 3.4.10). We conclude with open questions and suggestions for future work in Section 3.5.

- We obtain a normal form for collisions in the tame case described by a set of degree sequences for (possibly incomplete) decompositions (Theorems 3.4.2 and 3.4.5).
- The (non)uniqueness of the parameters leads to an exact formula for the number of such collisions over a finite field with characteristic coprime to their degree (Theorem 3.4.9).
- We conclude with a fast algorithm for the number of decomposable polynomials of degree n over a finite field of characteristic coprime to n (Algorithm 3.4.10).

3.1 NOTATION AND PRELIMINARIES

> However contracted, that definition is
> the result of expanded meditation.
> — Herman Melville

A nonzero polynomial $f \in F[x]$ over a field F of characteristic $p \geqslant 0$ is *monic* if its leading coefficient $\operatorname{lc}(f)$ equals 1. We call f *original* if its graph contains the origin, that is, $f(0) = 0$. For $g, h \in F[x]$,

$$f = g \circ h = g(h) \in F[x] \tag{3.1.1}$$

is their *composition*. If $\deg g, \deg h \geqslant 2$, then (g, h) is a *decomposition* of f. A polynomial $f \in F[x]$ is *decomposable* if there exist such g and h, otherwise f is *indecomposable*. A decomposition (3.1.1) is *tame* if $p \nmid \deg g$, and f is *tame* if $p \nmid \deg f$.

Multiplication by a unit or addition of a constant does not change decomposability, since

$$f = g \circ h \iff af + b = (ag + b) \circ h$$

for all f, g, h as above and $a, b \in F$ with $a \neq 0$. In other words, the set of decomposable polynomials is invariant under this action of $F^\times \times F$ on $F[x]$. Furthermore, every decomposition (g, h) of a monic original f can be normalized by this action, by taking $a = \operatorname{lc}(h)^{-1} \in F^\times$, $b = -a \cdot h(0) \in F$, $g^* = g((x - b)a^{-1}) \in F[x]$, and $h^* = ah + b$. Then $f = g \circ h = g^* \circ h^*$ and g^* and h^* are monic original.

It is therefore sufficient to consider compositions $f = g \circ h$, where all three polynomials are monic original. For $n \geqslant 1$ and d a positive divisor of n, we write

$$\mathcal{P}_n(F) = \{f \in F[x] \colon f \text{ is monic original of degree } n\},$$

$$\mathcal{D}_n(F) = \{f \in \mathcal{P}_n : f \text{ is decomposable}\},$$
$$\mathcal{D}_{n,d}(F) = \{f \in \mathcal{P}_n : f = g \circ h \text{ for some } (g,h) \in \mathcal{P}_d \times \mathcal{P}_{n/d}\}. \quad (3.1.2)$$

We sometimes leave out F from the notation, when it is clear from the context, and have over a finite field $\mathbb{F}_q$ with q elements

$$\#\mathcal{P}_n(\mathbb{F}_q) = q^{n-1}. \quad (3.1.3)$$

It is well known that in a tame decomposition, g and h are uniquely determined by f and $\deg g$ and we have over $\mathbb{F}_q$ with $p \nmid n$

$$\#\mathcal{D}_{n,d}(\mathbb{F}_q) = q^{d+n/d-2}. \quad (3.1.4)$$

The set $\mathcal{D}_n$ of all decomposable polynomials of degree n admits the covering

$$\mathcal{D}_n = \bigcup_{\substack{d|n \\ 1<d<n}} \mathcal{D}_{n,d}. \quad (3.1.5)$$

In particular, $\mathcal{D}_n = \varnothing$ if n is prime. Our collisions turn up in the resulting inclusion-exclusion formula for $\#\mathcal{D}_n(\mathbb{F}_q)$ if n is composite.

Let $N = \{1 < d < n : d \mid n\}$ be the set of nontrivial divisors of n. For $D \subseteq N$ a nonempty subset of size k, we define the set

$$\mathcal{D}_{n,D} = \bigcap_{d \in D} \mathcal{D}_{n,d}$$

of k-*collisions* and obtain from (3.1.5) the inclusion-exclusion formula

$$\#\mathcal{D}_n(\mathbb{F}_q) = \sum_{k \geqslant 1} (-1)^{k+1} \sum_{\substack{D \subseteq N \\ \#D=k}} \#\mathcal{D}_{n,D}. \quad (3.1.6)$$

For $\#D = 1$, the size of $\mathcal{D}_{n,D}$ is given in (3.1.4). For $\#D = 2$, the central conceptual and computational tool is Ritt's Second Theorem as presented in Theorem 3.1.10 below.

For $f \in P_n(F)$ and $a \in F$, the *original shift* of f by a is

$$f^{[a]} = (x - f(a)) \circ f \circ (x + a) \in \mathcal{P}_n(F).$$

Original shifting defines a group action of the additive group of F on $\mathcal{P}_n(F)$. The following lemma describes its stabilizers and orbits in the tame case.

Lemma 3.1.7. *Let $n \geqslant 1$, coprime to the characteristic of F, and $f \in \mathcal{P}_n$.*

(i) The stabilizer of f under original shifting is F if $n = 1$ and $\{0\}$ otherwise.

(ii) For $F = \mathbb{F}_q$ a finite field with q elements, the orbit of f under original shifting has size 1 if $n = 1$ and size q otherwise.

Proof. (i) If $n = 1$ then $f = x$ and $f^{[a]} = x$ for all $a \in F$. Otherwise, the coefficient of x^{n-1} in $f^{[a]}$ is $na + f_{n-1}$. Since $\operatorname{char}(F) \nmid n$, this is equal to f_{n-1} if and only if $a = 0$. (ii) follows from (i). □

Original shifting respect decompositions in the sense that for each decomposition (g, h) of f we have a decomposition $(g^{[h(a)]}, h^{[a]})$ of $f^{[a]}$, and vice versa. We denote $(g^{[h(a)]}, h^{[a]})$ as $(g, h)^{[a]}$.

Ritt (1922) presented two types of essential 2-collisions at degree n:

$$x^e \circ x^k w(x^e) = x^{ke} w^e(x^e) = x^k w^e \circ x^e,$$
$$T_d^*(x, z^e) \circ T_e^*(x, z) = T_{de}^*(x, z) = T_e^*(x, z^d) \circ T_d^*(x, z), \quad (3.1.8)$$

where $n = de$, $w \in F[x]$ of degree s, $d = s \cdot e + k$, T_d^* is the dth *Dickson polynomial of the first kind*, and $z \in F^\times = F \setminus \{0\}$. Then he proved that these are all possibilities up to composition with linear polynomials. This involved four unspecified linear functions, and it is not clear whether there is a relation between the first and the second type of example.

Von zur Gathen (2014b) presents a normal form for the decompositions in Ritt's Theorem under Zannier's assumption $g'(g^*)' \neq 0$ and the standard assumption $\gcd(e, d) = 1$. Without loss of generality, we use the *originalized* d*th Dickson polynomial* $T_d(x, z) = T_d^*(x, z) - T_d^*(0, z)$ which also satisfies (3.1.8). This normal form is unique and particularly simple if $p \nmid d$.

For coprime integers $d \geqslant 2$ and $e \geqslant 1$, we define the sets

$$\mathcal{E}_d^{(e)} = \begin{cases} \mathcal{P}_d & \text{for } e = 1, \\ \{x^k w^e \in \mathcal{P}_d : d = s \cdot e + k \text{ with } 1 \leqslant k < e \\ \quad \text{and } w \in \mathbb{F}_q[x] \text{ monic of degree } s\} & \text{otherwise,} \end{cases} \quad (3.1.9)$$

$$\mathcal{T}_d^{(e)} = \{T_d(x, z^e) \in \mathcal{P}_d : z \in \mathbb{F}_q^\times\}$$

of *exponential* and *trigonometric components*, respectively. We sometimes omit the exponent $e = 1$ from the notation. For $d < e$, we have $s = 0$, $k = d$ in (3.1.9), and therefore

$$\mathcal{E}_d^{(e)} = \{x^d\}.$$

For two sets $\mathcal{A}, \mathcal{B}$ of polynomials, we write $\mathcal{A} \circ \mathcal{B} = \{g \circ h : (g, h) \in \mathcal{A} \times \mathcal{B}\}$ for the compositions of $\mathcal{A} \times \mathcal{B}$ and $\mathcal{A}^{[F]} = \{f^{[a]} : f \in \mathcal{A}, a \in F\}$ for the original shifts of $\mathcal{A}$.

Theorem 3.1.10. *(Ritt's Second Theorem, Normal Form, tame case) Let $d > e \geqslant 2$ be coprime integers, and $n = de$ coprime to the characteristic of F. For $f \in \mathcal{D}_{n,\{d,e\}}$, we have either (i) or (ii) and (iii) is also valid.*

(i) (Exponential Case) There is a unique monic original $g \in \mathcal{E}_d^{(e)}$ and a unique $a \in F$ such that

$$f = (g \circ x^e)^{[a]}.$$

(ii) (Trigonometric Case) There is a unique monic original $T_n(x,z) \in \mathcal{T}_n$ *and a unique* $a \in F$ *such that*

$$f = T_n(x,z)^{[a]}.$$

(iii) If $e = 2$*, then case (ii) is included in case (i). If* $e \geqslant 3$*, they are mutually exclusive.*

Furthermore, we have

$$\mathcal{D}_{n,\{d,e\}} = \begin{cases} (\mathcal{E}_d^{(2)} \circ \mathcal{E}_2^{(d)})^{[F]} \supseteq \mathcal{T}_n^{[F]} & \text{if } e = 2, \\ (\mathcal{E}_d^{(e)} \circ \mathcal{E}_e^{(d)})^{[F]} \dot\cup \mathcal{T}_n^{[F]} & \text{otherwise,} \end{cases}$$
$$\#\mathcal{D}_{n,\{d,e\}} = q \cdot (q^{\lfloor d/e \rfloor} + (1 - \delta_{e,2})(q-1)),$$

where δ *denotes Kronecker's delta function.*

If $p \nmid n$, then the case where $\gcd(d,e) \neq 1$ is reduced to the previous one by the following result about the left and right greatest common divisors of decompositions. It was shown over algebraically closed fields by Tortrat (1988, Proposition 1); a more concise proof over $\mathbb{C}$ using Galois theory is due to Zieve & Müller (2008, Lemma 2.8). We use the version of von zur Gathen (2014b, Fact 6.1(i)), adapted to monic original polynomials.

Proposition 3.1.11. *Let* $d, e, d^*, e^* \geqslant 2$ *be integers and* $de = d^*e^*$ *coprime to the characteristic of* F*. Furthermore, let* $g \circ h = g^* \circ h^*$ *be monic original polynomials with* $\deg g = d$, $\deg h = e$, $\deg g^* = d^*$, $\deg h^* = e^*$, $\ell = \gcd(d, d^*)$*, and* $r = \gcd(e, e^*)$*. Then there are unique monic original polynomials* s *and* v *of degree* ℓ *and* r*, respectively, such that*

$$g = s \circ t, \qquad h = u \circ v,$$
$$g^* = s \circ t^*, \qquad h^* = u^* \circ v,$$

for unique monic original polynomials t, t^*, u, u^* *of degree* d/ℓ, d^*/ℓ, e/r, *and* e^*/r*, respectively.*

Together with Theorem 3.1.10, this determines $\mathcal{D}_{n,D}$ for $\#D = 2$ exactly if $p \nmid n$.

3.2 REFINEMENT OF FACTORIZATIONS

> Adrian Albert used to say that a theory is worth studying if it has at least three distinct good hard examples. Do not therefore define and study a new class of functions, the ones that possess left upper bimeasurably approximate derivatives, unless you can, at the very least, fulfill the good graduate student's immediate request: show me some that do and show me some that don't.
> — Paul Halmos

In the previous section, we dealt with 2-collisions of bi-decompositions $g \circ h = g^* \circ h^*$. In this section, we generalize them in two respects. First, every decomposition may have more than two components and second, more than two decompositions may collide.

Let $d = (d_1, d_2, \ldots, d_\ell)$ be an ordered factorization of the integer $n = d_1 \cdot d_2 \cdots d_\ell$ into ℓ divisors $d_i > 1$ of n, for $1 \leqslant i \leqslant \ell$. We define the set

$$\mathcal{D}_{n,d}(F) = \{f \in \mathcal{P}_n : \text{there are } g_i \in \mathcal{P}_{d_i} \text{ for } 1 \leqslant i \leqslant \ell \text{ with } f = g_1 \circ \cdots \circ g_\ell\}$$

of decomposable polynomials with *decomposition degree sequence* d of *length* $|d| = \ell$. This generalizes the set $\mathcal{D}_{n,d}$ as defined in (3.1.2) for a positive divisor d of n and we have $\mathcal{D}_{n,d} = \mathcal{D}_{n,d}$ for $d = (d, n/d)$. See Knopfmacher & Mays (2006) for a survey on enumerating and generating all ordered factorizations of a given n.

If $p \nmid n$, then the degree sequence determines the components uniquely and thus

$$\begin{aligned} \mathcal{D}_{n,d} &= \mathcal{P}_{d_1} \circ \mathcal{P}_{d_2} \circ \cdots \circ \mathcal{P}_{d_\ell}, \\ \#\mathcal{D}_{n,d}(\mathbb{F}_q) &= q^{-\ell + \sum_{1 \leqslant i \leqslant \ell} d_i}, \end{aligned} \tag{3.2.1}$$

where $d = (d_1, d_2, \ldots, d_\ell)$ is an ordered factorization of n.

For a nonempty set $D = \{d^{(1)}, d^{(2)}, \ldots, d^{(c)}\}$ of c distinct ordered factorizations of n, we define

$$\begin{aligned} \mathcal{D}_{n,D}(F) &= \bigcap_{d \in D} \mathcal{D}_{n,d} \\ &= \{f \in \mathcal{P}_n : \text{there are } g_i^{(k)} \in \mathcal{P}_{d_i^{(k)}} \text{ for } 1 \leqslant i \leqslant |d^{(k)}|, 1 \leqslant k \leqslant c \\ &\qquad \text{with } f = g_1^{(k)} \circ \cdots \circ g_{|d^{(k)}|}^{(k)}\}. \end{aligned}$$

In the tame case, the structure and size of $\mathcal{D}_{n,D}$ for $\#D = 1$ is described in (3.2.1). The goal of the remaining chapter is to determine it for $\#D > 1$. In this section, we replace D by a *normalization* D^*, where all elements are suitable permutations of the *same* ordered factorization of n. Then, we define the *relation graph* of D^* that captures the degree sequences for polynomials in $\mathcal{D}_{n,D}$ (Section 3.3). Finally, we describe $\mathcal{D}_{n,D}$ as compositions of the trigonometric and exponential components defined in (3.1.9) and determine the (non)uniqueness of this composition (Section 3.4).

Let $d = (d_1, d_2)$ and $e = (e_1, e_2)$ be two distinct ordered factorizations of n with $\ell = \gcd(d_1, e_1)$ and $r = \gcd(d_2, e_2)$. We define $d^* = (\ell, d_1/\ell, d_2/r, r)$ and $e^* = (\ell, e_1/\ell, e_2/r, r)$, where we omit entries equal to 1. Then

$$\mathcal{D}_{n,\{d,e\}} = \mathcal{D}_{n,\{d^*,e^*\}}$$

by Proposition 3.1.11 ("$\subseteq$") and a direct computation ("$\supseteq$"). Furthermore, e^* is a permutation of d^* since $\gcd(d_1/\ell, e_1/\ell) = 1 = \gcd(d_2/r, e_2/r)$ and thus $d_1/\ell = e_2/r$, $d_2/r = e_1/\ell$. In the tame case, this yields

$$\mathcal{D}_{n,\{d,e\}} = \mathcal{P}_\ell \circ \mathcal{D}_{n/(\ell r),\{(d_1/\ell, d_2/r),(d_2/r, d_1/\ell)\}} \circ \mathcal{P}_r$$

due to the absence of equal-degree collisions. We generalize this procedure to two ordered factorizations of arbitrary, possibly distinct, lengths.

Let us introduce some notation for an ordered factorization $d = (d_1, d_2, \ldots, d_\ell)$ of n. A *refinement* of d is an ordered factorization $d^* = (d^*_{11}, \ldots, d^*_{1m_1}, d^*_{21}, \ldots, d^*_{2m_2}, \ldots, d^*_{\ell 1}, \ldots, d^*_{\ell m_\ell})$ of n with $d_i = \prod_{1 \leqslant k \leqslant m_i} d^*_{ik}$ for all $1 \leqslant i \leqslant \ell$ and we write $d^* \mid d$. A refinement of d, where all entries are primes is called *complete*. Refinement defines a partial order on all ordered factorizations of n. Every complete refinement is minimal and the trivial factorization (n) is the unique maximum. For $d^* \mid d$, we have directly

$$\mathcal{D}_{n,d} \supseteq \mathcal{D}_{n,d^*}. \tag{3.2.2}$$

We call the underlying multiset of divisors $\underline{d} = \{d_1, d_2, \ldots, d_\ell\}$ the *support* of d. Two ordered factorizations $d = (d_1, \ldots, d_\ell)$ and $e = (e_1, \ldots, e_\ell)$ of n with the same support define a permutation $\sigma = \sigma(d, e)$ of the indices $1, 2, \ldots, \ell$ via

$$d_i = e_{\sigma(i)} \tag{3.2.3}$$

for $1 \leqslant i \leqslant \ell$. We require

$$\sigma(i) < \sigma(j) \text{ for all } i < j \text{ with } d_i = d_j$$

to make σ unique. In other words, σ has to preserve the order of repeated divisors. If we have, even more restrictively,

$$\sigma(i) < \sigma(j) \text{ for all } i < j \text{ with } \gcd(d_i, d_j) > 1, \tag{3.2.4}$$

then we call d and e *aligned*.

Complete refinements d^* of d and e^* of e, respectively, are aligned and we derive from (3.2.2)

$$\mathcal{D}_{n,\{d,e\}} \supseteq \mathcal{D}_{n,\{d^*,e^*\}}. \tag{3.2.5}$$

But, we ask for aligned refinements that yield equality in (3.2.5). A basic step to this end is described by the following lemma.

Lemma 3.2.6. *Let n be coprime to the characteristic of F, $d = (d_1, \ldots, d_\ell)$ and $e = (e_1, \ldots, e_m)$ ordered factorizations of n, and $g_1 \circ g_2 \circ \cdots \circ g_\ell = h_1 \circ h_2 \circ \cdots \circ h_m$ two decompositions of $f \in \mathcal{P}_n$ with degree sequences d and e, respectively. For all $1 \leqslant i \leqslant \ell$ and $1 \leqslant j \leqslant m$ with*

$$\gcd(d_1 \cdot \ldots \cdot d_{i-1} \cdot d_i, e_1 \cdot \ldots \cdot e_{j-1}) = \gcd(d_1 \cdot \ldots \cdot d_{i-1}, e_1 \cdot \ldots \cdot e_{j-1} \cdot e_j), \quad (3.2.7)$$

we have unique monic original polynomials u, v, u^*, *and* v^* *of degree* $c = \gcd(d_i, e_j)$, d_i/c, c, *and* e_j/c, *respectively, such that*

$$g_i = u \circ v \text{ and } h_j = u^* \circ v^*. \quad (3.2.8)$$

Therefore, f *has decomposition degree sequences* $d^* = (d_1, \ldots, d_{i-1}, c, d_i/c, d_{i+1}, \ldots, d_\ell) \mid d$ *if* $1 < c < d_i$, *and* $e^* = (e_1, \ldots, e_{j-1}, c, e_j/c, e_{j+1}, \ldots, e_\ell) \mid e$ *if* $1 < c < e_j$.

Proof. Let $1 \leqslant i \leqslant \ell$ and $1 \leqslant j \leqslant m$ such that (3.2.7) holds and define $G = g_1 \circ \cdots \circ g_{i-1}$ and $H = h_1 \circ \cdots \circ h_{j-1}$ of degree D_{i-1} and E_{j-1}, respectively, where an empty decomposition is equal to x. Then Proposition 3.1.11 applied to the bi-decompositions

$$G \circ (g_i \circ \cdots \circ g_\ell) = H \circ (h_j \circ \cdots \circ h_m) \quad (3.2.9)$$

guarantees for the left components the existence of unique monic original s, t, and t^* with degrees $b = \gcd(D_{i-1}, E_{j-1})$, $D'_{i-1} = D_{i-1}/b$, and $E'_{j-1} = E_{j-1}/b$, respectively, such that

$$G = s \circ t \text{ and } H = s \circ t^*, \quad (3.2.10)$$

$$\gcd(D'_{i-1}, E'_{j-1}) = 1. \quad (3.2.11)$$

Condition (3.2.7) provides $\gcd(D_{i-1} \cdot d_i, E_{j-1}) = \gcd(D_{i-1}, E_{j-1} \cdot e_j)$. We divide by b to find $\gcd(d_i, E'_{j-1}) = \gcd(D'_{i-1}, e_j)$. These gcds equal 1, since E'_{j-1} and D'_{i-1} are coprime, and in particular

$$\gcd(d'_i, E'_{j-1}) = \gcd(D'_{i-1}, e'_j) = 1 \quad (3.2.12)$$

for all $d'_i \mid d_i$ and $e'_j \mid e_j$.

We substitute (3.2.10) back into (3.2.9), cancel the common left component s, and consider the bi-decomposition

$$(t \circ g_i) \circ (g_{i+1} \circ \cdots \circ g_\ell) = (t^* \circ h_j) \circ (h_{j+1} \circ \cdots \circ h_m). \quad (3.2.13)$$

For the left components, we compute with (3.2.11) and (3.2.12)

$$\begin{aligned}\gcd(\deg(t \circ g_i), \deg(t^* \circ h_j)) &= \gcd(D'_{i-1} \cdot d_i, E'_{j-1} \cdot e_j) \\ &= \gcd(D'_{i-1}, E'_{j-1}) \cdot \gcd\left(\frac{D'_{i-1}}{\gcd(D'_{i-1}, E'_{j-1})}, \frac{e_j}{c}\right) \\ &\quad \cdot \gcd\left(\frac{d_i}{c}, \frac{E'_{j-1}}{\gcd(D'_{i-1}, E'_{j-1})}\right) \cdot \gcd(d_i, e_j) \\ &= c.\end{aligned}$$

Thus, Proposition 3.1.11 applied to the left components of (3.2.13) yields unique monic original τ, γ, τ^*, and η of degree c, $D'_{i-1}\,d_i/c$, c, and $E'_{j-1}\,e_j/c$, respectively, such that

$$\begin{aligned} t \circ g_i &= \tau \circ \gamma, \\ t^* \circ h_j &= \tau^* \circ \eta. \end{aligned} \tag{3.2.14}$$

For the right components of each collision in (3.2.14), we compute with (3.2.12)

$$\begin{aligned} \gcd(\deg g_i, \deg \gamma) &= \gcd(d_i, D'_{i-1}\,d_i/c) \\ &= \gcd(d_i, d_i/c) \cdot \gcd(c, D'_{i-1}) = d_i/c, \\ \gcd(\deg h_j, \deg \eta) &= \gcd(e_j, E'_{j-1}\,e_j/c) \\ &= \gcd(e_j, e_j/c)\,\gcd(c, E'_{j-1}) = e_j/c, \end{aligned}$$

respectively. Thus, a final application of Proposition 3.1.11 to (3.2.14) yields the unique decompositions of g_i and h_j claimed in (3.2.8). □

The two refinements d^* and e^* defined in Lemma 3.2.6 have the common element c and describe the same collisions as $d = (d_1, \ldots, d_\ell)$ and $e = (e_1, \ldots, e_m)$ do. This is the basic step in the following procedure to find refinements having common support and describing the same collisions.

We build an $(\ell+1) \times (m+1)$-matrix $C^{(0)}$ of positive integers by taking an $\ell \times m$-matrix of all 1's at the top left and adding a border column and row, at right and bottom, respectively, containing d and e, respectively, plus 1 at position $(\ell+1, m+1)$, that is

$$C^{(0)} = \begin{pmatrix} 1 & \ldots & 1 & d_1 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \ldots & 1 & d_\ell \\ e_1 & \ldots & e_m & 1 \end{pmatrix} = (c^{(0)}_{i,j})_{\substack{1 \leqslant i \leqslant \ell+1 \\ 1 \leqslant j \leqslant m+1}} \in \mathbb{N}^{(\ell+1)\times(m+1)}. \tag{3.2.15}$$

We extend this recursively to a sequence of integer matrices $C^{(k)} \in \mathbb{N}^{(\ell+1)\times(m+1)}$ for $1 \leqslant k \leqslant \ell m$, by writing $k = (i-1)m + j$ with unique $1 \leqslant i \leqslant \ell$ and $1 \leqslant j \leqslant m$, computing $c = \gcd(c^{(k-1)}_{i,m+1}, c^{(k-1)}_{\ell+1,j})$, and defining $C^{(k)}$ as $C^{(k-1)}$ with the three modifications

$$c^{(k)}_{i,j} \leftarrow c,\ c^{(k)}_{i,m+1} \leftarrow c^{(k-1)}_{i,m+1}/c, \text{ and } c^{(k)}_{\ell+1,j} \leftarrow c^{(k-1)}_{\ell+1,j}/c. \tag{3.2.16}$$

If $c = 1$, we have $C^{(k)} = C^{(k-1)}$. Otherwise, the matrices $C^{(k)}$ and $C^{(k-1)}$ differ at the positions (i,j), $(i, m+1)$, and $(\ell+1, j)$ viz

$$C^{(k)} = \begin{pmatrix} c & c^{(k-1)}_{i,m+1}/c \\ c^{(k-1)}_{\ell+1,j}/c & \end{pmatrix}, \quad C^{(k-1)} = \begin{pmatrix} 1 & c^{(k-1)}_{i,m+1} \\ c^{(k-1)}_{\ell+1,j} & \end{pmatrix} \tag{3.2.17}$$

and are identical at all other positions.

Every matrix $C^{(k)}$ for $0 \leqslant k \leqslant \ell m$, provides two ordered factorizations $d^{(k)}$ and $e^{(k)}$. For $d^{(k)}$, we read $C^{(k)}$ row-by-row skipping entries equal to 1 and skipping the bottom row. Similarly for $e^{(k)}$, we read $C^{(k)}$ column-by-column skipping entries equal to 1 and skipping the right column. We have $d^{(0)} = d$, $e^{(0)} = e$ by (3.2.15) and $d^{(k)} \mid d^{(k-1)}$, $e^{(k)} \mid e^{(k-1)}$ for $1 \leqslant k \leqslant \ell m$. We call the final $d^{(\ell m)}$ the *refinement of* d *by* e, denoted by $d /\!\!/ e$, and also have $e^{(\ell m)} = e /\!\!/ d$, see Proposition 3.2.19 (iii). Algorithm 3.2.18 summarizes the outlined procedure and returns $d /\!\!/ e$ and $e /\!\!/ d$. These refinements are aligned and describe the same collisions as d and e do, see Proposition 3.2.19 (iv).

Algorithm 3.2.18: Refine d by e and e by d

Input: two ordered factorizations $d = (d_1, \dots, d_\ell)$ and $e = (e_1, \dots, e_m)$ of n

Output: two aligned refinements $d^* \mid d$ and $e^* \mid e$

$k \leftarrow 0$ and $C^{(0)} = (c^{(0)}_{i,j})_{\substack{1 \leqslant i \leqslant \ell+1 \\ 1 \leqslant j \leqslant m+1}} \leftarrow \begin{pmatrix} 1 & \dots & 1 & d_1 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \dots & 1 & d_\ell \\ e_1 & \dots & e_m & 1 \end{pmatrix}$

for $i = 1, \dots, \ell$ **do**
  for $j = 1, \dots, m$ **do**
    $k \leftarrow k+1$ and $C^{(k)} \leftarrow C^{(k-1)}$ /* $k = (i-1) \cdot m + j$ */
    $c \leftarrow \gcd(c^{(k-1)}_{i,m+1}, c^{(k-1)}_{\ell+1,j})$
    $c^{(k)}_{i,j} \leftarrow c$, $c^{(k)}_{i,m+1} \leftarrow c^{(k-1)}_{i,m+1}/c$, and $c^{(k)}_{\ell+1,j} \leftarrow c^{(k-1)}_{\ell+1,j}/c$
  end
end

/* read $C^{(\ell m)}$ row-by-row skipping entries equal to 1 and skipping the bottom row */

$d^* \leftarrow d^{(\ell m)} = (c^{(\ell m)}_{i,j} \text{ if } c^{(\ell m)}_{i,j} > 1)_{\substack{1 \leqslant k \leqslant \ell(m+1) \\ k=(i-1)(m+1)+j \\ 1 \leqslant i \leqslant \ell, 1 \leqslant j \leqslant m+1}}$

/* read $C^{(\ell m)}$ column-by-column skipping entries equal to 1 and skipping the right column */

$e^* \leftarrow e^{(\ell m)} = (c^{(\ell m)}_{i,j} \text{ if } c^{(\ell m)}_{i,j} > 1)_{\substack{1 \leqslant k \leqslant m(\ell+1) \\ k=(j-1)(\ell+1)+i \\ 1 \leqslant j \leqslant m, 1 \leqslant i \leqslant \ell+1}}$

return d^*, e^*

Proposition 3.2.19. *Let* $d = (d_1, \dots, d_\ell)$ *and* $e = (e_1, \dots, e_m)$ *be two ordered factorizations of* n *and* $C^{(k)} \in \mathbb{N}^{(\ell+1)\times(m+1)}$, $0 \leqslant k \leqslant \ell m$, *the sequence of integer matrices defined by* (3.2.15) *and* (3.2.16). *Then the following holds.*

(i) *For* $1 \leqslant i \leqslant \ell$, $1 \leqslant j \leqslant m$, *and* $0 \leqslant k \leqslant \ell m$, *the product of all entries in the* i*th row of* $C^{(k)}$ *is* d_i *and the product of all entries in the* j*th column of* $C^{(k)}$ *is* e_j.

(ii) *For* $1 \leqslant i < i' \leqslant \ell + 1$, $1 \leqslant j' < j \leqslant m + 1$, *and* $(i-1)m + j' \leqslant k \leqslant \ell m$, *we have*

$$\gcd(c_{i,j}^{(k)}, c_{i',j'}^{(k)}) = 1. \tag{3.2.20}$$

Furthermore, every entry in the bottom row and every entry in the right column of the final $C^{(\ell m)}$ *is equal to* 1.

(iii) *Algorithm 3.2.18 works as specified. Furthermore, on input* d *and* e, *it returns* $d /\!\!/ e$ *and* $e /\!\!/ d$ *using* ℓm gcd*-computations and* $2\ell m$ *exact divisions on integers* $\leqslant n$.

(iv) *We have* $\mathcal{D}_{n,\{d,e\}} = \mathcal{D}_{n,\{d/\!/e,e\}} = \mathcal{D}_{n,\{d,e/\!/d\}} = \mathcal{D}_{n,\{d/\!/e,e/\!/d\}}$.

Proof. (i) For $k = 0$, the claim follows from (3.2.15) and we proceed inductively. For $k > 0$, we write $k = (i'-1)m + j'$ with $1 \leqslant i' \leqslant \ell$ and $1 \leqslant j' \leqslant m$. Then the i'th row in $C^{(k)}$ is obtained from the i'th row in $C^{(k-1)}$ by replacing entries equal to 1 and $c_{i',m+1}^{(k-1)}$ by c and $c_{i',m+1}^{(k-1)}/c$, respectively as shown in (3.2.17). Similarly, the j'th column in $C^{(k)}$ is obtained from the j'th column in $C^{(k-1)}$ by replacing entries equal to 1 and $c_{\ell+1,j'}^{(k-1)}$ by c and $c_{\ell+1,j'}^{(k-1)}/c$, respectively. These are the only substitutions. They leave the product of all entries in the ith row and the product of all entries in the jth column unchanged and thus equal to d_i and e_j, respectively.

(ii) Let $k_0 = (i-1)m + j'$. Then $\gcd(c_{i,m+1}^{(k_0)}, c_{\ell+1,j'}^{(k_0)}) = 1$ since the substitution (3.2.16) factors out $\gcd(c_{i,m+1}^{(k_0-1)}, c_{\ell+1,j'}^{(k_0-1)})$ when defining $C^{(k_0)}$. We have $j' < j$ and $k_0 \leqslant k$, thus $c_{i,j}^{(k)}$ is a divisor of $c_{i,m+1}^{(k_0)}$. Also, $i < i'$ and $k_0 \leqslant k$ yield $c_{i',j'}^{(k)} \mid c_{\ell+1,j'}^{(k_0)}$. This proves (3.2.20).

For all $0 \leqslant k \leqslant \ell m$, we have 1 at the position $(\ell + 1, m + 1)$ of $C^{(k)}$. We denote the top left $\ell \times m$-submatrix of $C^{(\ell m)}$ by $D = (c_{i,j}^{(\ell m)})_{1 \leqslant i \leqslant \ell, 1 \leqslant j \leqslant m}$, the bottom row of $C^{(\ell m)}$, excluding the 1 at position $(\ell + 1, m + 1)$, by $B = (c_{\ell+1,j}^{(\ell m)})_{1 \leqslant j \leqslant m}$, and the right column of $C^{(\ell m)}$, again excluding the 1 at position $(\ell + 1, m + 1)$, by $R = (c_{i,m+1}^{(\ell m)})_{1 \leqslant i \leqslant \ell}$, that is

$$C^{(\ell m)} = \begin{pmatrix} D & R \\ B & 1 \end{pmatrix}.$$

Let D, R, B denote the product of all entries in D, R, B, respectively. From (i), we have $n = DR = DB$, thus $R = B$. Taking $i' = \ell + 1$, $j = m + 1$, and $k = \ell m$ in (3.2.20) we find that every entry in R is coprime to every entry in B. Thus, $\gcd(B, R) = 1$ and we conclude $R = B = 1$.

(iii) The outputs d^* and e^* are refinements of d and e, respectively, by (i). The common support of d^* and e^* is the multiset of entries in

$D^{(\ell m)}$ that are greater than 1 by (ii). We now show that d^* and e^* are aligned.

Assume that all entries of $D^{(\ell m)}$ are greater than 1 and therefore $\underline{d^*} = \underline{e^*} = \{c_{i,j}^{(\ell m)} : 1 \leqslant i \leqslant \ell, 1 \leqslant j \leqslant m\}$ is a multiset of size ℓm. We define a permutation σ on $\{1, \ldots, \ell m\}$ via $\sigma(k) = (j-1)\ell + i$, where $k = (i-1)m + j$ with $1 \leqslant i \leqslant \ell$, $1 \leqslant j \leqslant m$ and have

$$c_{i,j}^{(\ell m)} = d_k^* = e_{\sigma(k)}^*.$$

Let $k < k' = (i'-1)m + j' \leqslant \ell m$ with $1 \leqslant i' \leqslant \ell$, $1 \leqslant j' \leqslant m$. We prove that $\sigma(k) > \sigma(k')$ implies $\gcd(d_k^*, d_{k'}^*) = 1$. The conditions on k and k' are equivalent to $i < i'$ and $j > j'$ and the claim follows from (3.2.20).

In the general case, where $D^{(\ell m)}$ may contain 1's, the restriction of σ from above to indices $k = (i-1)m + j$ with $c_{i,j}^{(\ell m)} > 1$ provides the required permutation.

We have $d^* = d /\!\!/ e$ by definition. We check directly that if the order of the inputs to the algorithm is reversed, then the final state is the transpose of $C^{(\ell m)}$. Thus $e /\!\!/ d = e^*$.

Finally, the only arithmetic costs are the gcd-computations in step 5 and the integer divisions in step 6.

(iv) We begin with the first equality and show inductively

$$\mathcal{D}_{n,\{d^{(k-1)},e\}} = \mathcal{D}_{n,\{d^{(k)},e\}} \tag{3.2.21}$$

for all $1 \leqslant k \leqslant \ell m$.

Let $k = (i-1)m + j$ with $1 \leqslant i \leqslant \ell$, $1 \leqslant j \leqslant m$. If $c = 1$ in (3.2.16), then $d^{(k)} = d^{(k-1)}$ and (3.2.21) holds trivially. Otherwise, $d^{(k)}$ is the proper refinement of $d^{(k-1)}$, where the entry $c_{i,m+1}^{(k-1)}$ in $d^{(k-1)}$ is replaced by the pair $(c, c_{i,m+1}^{(k-1)}/c)$. Thus, we have "$\supseteq$" in (3.2.21) by (3.2.5).

For "$\subseteq$", we denote by D the denote the top left $i \times j$-submatrix of $C^{(k-1)}$, by R the top right $(i-1) \times (m+1-j)$-submatrix of $C^{(k-1)}$, and by B the lower left $(\ell+1-i) \times (j-1)$-submatrix of $C^{(k-1)}$. This yields the partition

$$C^{(k-1)} = \left(\begin{array}{cc|c} \multicolumn{2}{c|}{D} & R \\ \hline & & 1' \quad c_{i,m+1}^{(k-1)} \\ \hline B & \begin{matrix} 1 \\ c_{\ell+1,j}^{(k-1)} \end{matrix} & * \end{array}\right),$$

where $1'$ and 1 denote the row and the column vector consisting of $m-j$ and $\ell-i$ ones, respectively. Let D, R, B denote the product of all entries in D, R, B, respectively. We have $\gcd(R, B) = \gcd(c_{i,m+1}^{(k-1)}, B) =$

$\gcd(R, c_{\ell+1,j}^{(k-1)}) = 1$ by (ii). Let i^* denote the index of $c_{i,m+1}^{(k-1)}$ in $d^{(k-1)}$ and j^* denote the index of $c_{\ell+1,j}^{(k-1)}$ in $e^{(k-1)}$. Then

$$\begin{aligned}
&\gcd(d_1^{(k-1)} \cdots d_{i^*-1}^{(k-1)} d_{i^*}^{(k-1)}, e_1^{(k-1)} \cdots e_{j^*-1}^{(k-1)}) \\
&= \gcd(DBc_{\ell+1,j}^{(k-1)}, DR) = D = \gcd(DB, DRc_{i,m+1}^{(k-1)}) \\
&= \gcd(d_1^{(k-1)} \cdots d_{i^*-1}^{(k-1)}, e_1^{(k-1)} \cdots e_{j^*-1}^{(k-1)}, e_{j^*}^{(k-1)})
\end{aligned}$$

and we apply Lemma 3.2.6 with $d = d^{(k-1)}$, $e = e^{(k-1)}$, $i = i^*$, and $j = j^*$ to find "$\subseteq$" in (3.2.21).

Finally, interchanging the rôles of d and e yields

$$\begin{aligned}
\mathcal{D}_{n,\{d,e\}} &= \mathcal{D}_{n,\{d/\!/e,e\}} = \mathcal{D}_{n,\{d,e/\!/d\}} \\
&= \mathcal{D}_{n,\{d/\!/e,e\}} \cap \mathcal{D}_{n,\{d,e/\!/d\}} = \mathcal{D}_{n,\{d/\!/e,e/\!/d,d,e\}} = \mathcal{D}_{n,\{d/\!/e,e/\!/d\}},
\end{aligned}$$

where the last equality follows from the fact that the refined composition degree sequence $d /\!/ e$ implies d and similarly $e /\!/ d$ implies e. □

For squarefree n this is similar to the computation of a *coprime basis* (or gcd-free basis) for $\underline{d} \cup \underline{e}$, if we keep duplicates and the order of factors; see Bach & Shallit (1997, Section 4.8). For squareful n, the factors with gcd > 1 require additional attention.

Example 3.2.22. Let $n = 7! = 5040$. On input $d = (12, 420)$ and $e = (14, 360)$, Algorithm 3.2.18 runs through the states

$$C^{(0)} = \begin{pmatrix} 1 & 1 & 12 \\ 1 & 1 & 420 \\ 14 & 360 & 1 \end{pmatrix}, \quad C^{(1)} = \begin{pmatrix} 2 & 1 & 6 \\ 1 & 1 & 420 \\ 7 & 360 & 1 \end{pmatrix},$$

$$C^{(2)} = \begin{pmatrix} 2 & 6 & 1 \\ 1 & 1 & 420 \\ 7 & 60 & 1 \end{pmatrix}, \quad C^{(3)} = \begin{pmatrix} 2 & 6 & 1 \\ 7 & 1 & 60 \\ 1 & 60 & 1 \end{pmatrix}, \quad C^{(4)} = \begin{pmatrix} 2 & 6 & 1 \\ 7 & 60 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

and provides as aligned refinements

$$\begin{aligned}
d /\!/ e &= (2, 6, 7, 60) \mid d, \\
e /\!/ d &= (2, 7, 6, 60) \mid e.
\end{aligned}$$

If the characteristic of F is greater than 7, then any $f \in \mathcal{D}_{n,\{d,e\}}$ has a unique decomposition $f = a \circ g \circ b$ with $a \in \mathcal{P}_2$, $g \in \mathcal{D}_{42,\{(6,7),(7,6)\}}$, and $b \in \mathcal{P}_{60}$ due to the absence of equal-degree collisions.

Algorithm 3.2.18 returns the "coarsest" aligned refinements of two given ordered factorizations. Two ordered factorizations that are already aligned remain unchanged.

Lemma 3.2.23. *For two ordered factorizations* d *and* e *of* n*, the following are equivalent.*

(i) d *and* e *are aligned.*

(ii) $\mathsf{d} /\!\!/ \mathsf{f}$ *and* $\mathsf{e} /\!\!/ \mathsf{f}$ *are aligned for all ordered factorizations* f *of* n*.*

(iii) $\mathsf{d} /\!\!/ \mathsf{e} = \mathsf{d}$ *and* $\mathsf{e} /\!\!/ \mathsf{d} = \mathsf{e}$*.*

Proof. Assume that $\mathsf{d} = (d_1, \dots, d_\ell)$ and $\mathsf{e} = (e_1, \dots, e_\ell)$ are aligned and $\sigma = \sigma(\mathsf{d}, \mathsf{e})$ is the unique permutation on $\{1, \dots, \ell\}$ satisfying (3.2.3) and (3.2.4). We extend σ to $\{1, \dots, \ell+1\}$ via $\sigma(\ell+1) = \ell+1$.

On input d and e, Algorithm 3.2.18 begins with the state

$$C^{(0)} = \begin{pmatrix} 1 & \dots & 1 & d_1 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \dots & 1 & d_\ell \\ e_1 & \dots & e_\ell & 1 \end{pmatrix} = \begin{pmatrix} 1 & \dots & 1 & e_{\sigma(1)} \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \dots & 1 & e_{\sigma(\ell)} \\ e_1 & \dots & e_\ell & 1 \end{pmatrix}$$

and terminates with the state $C^{(\ell^2)}$ defined by

$$c_{i,j}^{(\ell^2)} = \begin{cases} d_i = e_{\sigma(i)} & \text{if } j = \sigma(i), \\ 1 & \text{otherwise,} \end{cases}$$

for all $1 \leqslant i, j \leqslant \ell+1$. Thus, it returns d and e and (iii) follows.

Let $\mathsf{f} = (f_1, \dots, f_m)$ be an ordered factorization of n. On input d, f and e, f, respectively, the initial state of Algorithm 3.2.18 is

$$\begin{pmatrix} 1 & \dots & 1 & d_1 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \dots & 1 & d_\ell \\ f_1 & \dots & f_m & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & \dots & 1 & e_1 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \dots & 1 & e_\ell \\ f_1 & \dots & f_m & 1 \end{pmatrix}$$

respectively. Let C and D, respectively, denote the final state, respectively.

We define the permutation τ of the indices $I = \{1, \dots, \ell+1\} \times \{1, \dots, m\}$ of C by $\tau(i,j) = (\sigma(i), j)$ for $1 \leqslant i \leqslant \ell+1$, $1 \leqslant j \leqslant m+1$. We take the lexicographic order on I, corresponding to reading row-by-row, and claim

$$c_{i,j} = d_{\tau(i,j)}, \tag{3.2.24}$$

$$\gcd(c_{i,j}, c_{i'j'}) = 1, \tag{3.2.25}$$

for all $(i,j), (i',j') \in I$ with $(i,j) < (i',j')$ and $(i,j) > \tau(i',j')$.

Assume for contradiction that (i,j) is the minimal index where some prime p divides $d_{\sigma(i),j}$, but not $c_{i,j}$. The product of all elements in the ith row of C is d_i and the product of all elements in the $\sigma(i)$th row of D, namely $e_{\sigma(i)} = d_i$. There is therefore some column index j' such that $p \mid d_{i,j'}$ and $j' > j$ by assumption. Similarly, there is some

row index i' such that $p \mid d_{i',j}$. This is a contradiction to Proposition 3.2.19 (ii) and proves (3.2.24). Similarly, if there is some prime dividing c, but not d.

The conditions on (i,j) and (i',j') imply $\sigma(i) > \sigma(i')$. But then $c_{i,j} \mid d_i$ and $c_{i',j'} \mid d_{i'}$ and $\gcd(d_i, d_{i'}) = 1$ since $\sigma(i) > \sigma(i')$ and $i < i'$. This proves (3.2.25).

Together, if we restrict τ to the indices with $c_{i,j} > 1$, we obtain a map from the indices of $d /\!\!/ f$ to the indices of $e /\!\!/ f$ satisfying (3.2.3) and (3.2.4) and (ii) follows.

Conversely, we assume (ii). Then $d /\!\!/ (n) = d$ and $e /\!\!/ (n) = e$ are aligned and (i) follows.

Finally, we assume that Algorithm 3.2.18 returns d and e on input d and e. Then they are aligned by Proposition 3.2.19 (iii) and (i) follows.

□

Given a set D with more than two ordered factorizations, we repeatedly replace pairs $d, e \in D$ by $d /\!\!/ e$ and $e /\!\!/ d$, respectively, until we reach a set D^* of refinements invariant under this operation. We call a nonempty set D of ordered factorizations *normalized* if all elements are pairwise aligned. A normalized D^* with $\mathcal{D}_{n,D^*} = \mathcal{D}_{n,D}$ is called a *normalization* of D.

This process terminates by Lemma 3.2.23. The result depends on the order of the applied refinements, but any order ensures the desired properties.

Proposition 3.2.26. *Let n be a positive integer and D a set of c ordered factorizations of n. There is a set D^* of at most c ordered factorizations of n with the following properties.*

(i) *D^* is normalized.*

(ii) *$\mathcal{D}_{n,D^*} = \mathcal{D}_{n,D}$.*

(iii) *D^* can be computed from D with at most $c(c-1)/2$ calls to Algorithm 3.2.18.*

Proof. For $c = 1$, we have $D = \{d\}$ and $D^* = \{d\}$ satisfies all claims.

For $c = 2$, we have $D = \{d, e\}$ for ordered factorizations $d \neq e$, and $D^* = \{d /\!\!/ e, e /\!\!/ d\}$ satisfies all claims by Proposition 3.2.19.

Let $c > 2$ and $D = \{d^{(1)}, \dots, d^{c}\}$. By induction assumption, we can assume all $d^{(i)}$ for $1 \leqslant i < c-1$ be pairwise aligned. Let $d^{(c)} = f$ and $D^* = \{d^{(1)} /\!\!/ f, d^{(2)} /\!\!/ f, \dots, d^{(c-1)} /\!\!/ f, f /\!\!/ d^{(1)}\}$. Clearly $\mathcal{D}_{n,D} = \mathcal{P}_{n,D^*}$ and it remains to show that all elements of D^* are pairwise aligned.

By construction, we have $d^{(1)} /\!\!/ f$ aligned with $f /\!\!/ d^{(1)}$ and by transitivity of alignedness the (ii) suffices.

□

We call any D^* satisfying Proposition 3.2.26(i)-(ii) a *normalization* of D. Also, we call D *normalized*, if $D = D^*$. For a normalized $D = \{d^{(k)} : 1 \leqslant k \leqslant c\}$, we have the same support $\underline{d^{(k)}}$ for all $1 \leqslant k \leqslant c$ and call this multiset the *support* of D, denoted by $\underline{D}$.

Example 3.2.27. We add the ordered factorization $f = (20, 252)$ to $D = \{d, e\}$ from Example 3.2.22. Then the normalization obtained via the process described above consists of

$$\begin{aligned} d^* &= (d /\!\!/ e) /\!\!/ f = (2,2,3,7,5,12)\,, \\ e^* &= (e /\!\!/ d) /\!\!/ f = (2,7,2,3,5,12)\,, \\ f^* &= f /\!\!/ (d /\!\!/ e) = (2,2,5,3,7,12)\,. \end{aligned} \tag{3.2.28}$$

For the last refinement, Algorithm 3.2.18 runs through the states

$$C^{(0)} = \begin{pmatrix} 1 & 1 & 1 & 1 & 20 \\ 1 & 1 & 1 & 1 & 252 \\ 2 & 6 & 7 & 60 & 1 \end{pmatrix}, C^{(4)} = \begin{pmatrix} 2 & 2 & 1 & 5 & 1 \\ 1 & 1 & 1 & 1 & 252 \\ 1 & 3 & 7 & 12 & 1 \end{pmatrix},$$

$$C^{(8)} = \begin{pmatrix} 2 & 2 & 1 & 5 & 1 \\ 1 & 3 & 7 & 12 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

If the characteristic of F is greater than 7, than any $f \in \mathcal{P}_{n,\{d,e,f\}} = \mathcal{P}_{n,\{d^*,e^*,f^*\}}$ has a unique decomposition $f = a \circ g \circ b$ with $a \in \mathcal{P}_2$, $g \in \mathcal{D}_{210,\{(2,3,7,5),(7,2,3,5),(2,5,3,7)\}}$, and $b \in \mathcal{P}_{12}$ due to the absence of equal-degree collisions. The support of the normalized $\{d^*, e^*, f^*\}$ is the multiset $\{2, 2, 3, 5, 7, 12\}$.

3.3 RELATION GRAPH OF D

> Mathematicians love to build bridges between apparently disconnected fields, hoping to get a better perspective of both.
>
> — Andrew Granville

For an ordered factorization $d = (d_1, d_2, \ldots, d_\ell)$ of n, we define its *relation graph* as the (vertex-)labeled directed graph G_d with

- vertices $1, 2, \ldots, \ell$,
- label d_i attached to vertex i for $1 \leqslant i \leqslant \ell$,
- and directed edges $i \to j$ for all $1 \leqslant i < j \leqslant \ell$.

The underlying undirected graph is complete and therefore G_d is a *tournament*. For a tournament G, the following are equivalent.

- G is *transitive*, that is every path $i \to j \to k$ for vertices i, j, k of G implies an edge $i \to k$ in G.

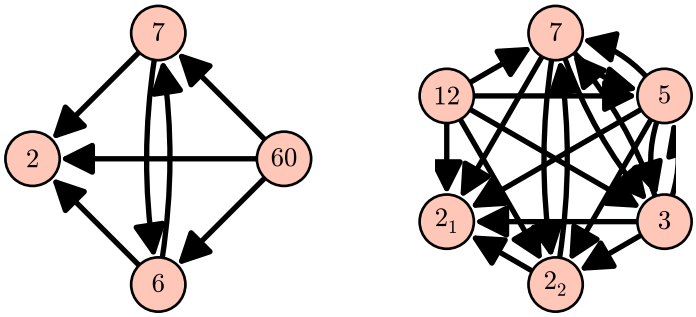

Figure 3.3.1: Relation graphs of Examples 3.2.22 and 3.2.27; in the latter, 2_i denotes the ith 2 in each ordered factorization for $i = 1, 2$.

- G has a unique *Hamiltonian* path, that is a path in G that visits every vertex of G exactly once.

A relation graph satisfies these conditions. The transitivity of "$<$" in the specification of the edges implies the transitivity of G_d and $1 \to 2 \to \cdots \to \ell$ is its unique Hamiltonian path.

Now, let $D = \{d^{(1)}, d^{(2)}, \ldots, d^{(c)}\}$ be a normalized set of c ordered factorizations ordered lexicographically. We start with the relation graph $G_{d^{(1)}}$ and for each $k > 1$ add directed edges $i \to j$ for all $1 \leqslant i, j \leqslant \ell$ with $\sigma(d^{(1)}, d^{(k)})(i) < \sigma(d^{(1)}, d^{(k)})(j)$. In other words, we build the union of all G_d for $d \in D$, where we identify vertices via the σ (and choose labels according to $d^{(1)}$). The resulting graph is called the *relation graph* of D, denoted as G_D. The underlying undirected graph is still complete, but since G_D may contain bidirectional edges this may be no tournament. Furthermore, it may be intransitive and contain several Hamiltonian paths. See Figure 3.3.1 for the relation graphs of Example 3.2.22 and Example 3.2.27.

A Hamiltonian path $p = v_1 \to v_2 \to \cdots \to v_\ell$ in a directed graph G with vertices $\{1, 2, \ldots\}$ defines a unique permutation σ_p of $\{1, 2, \ldots, \ell\}$ such that $\sigma_p(i) \to \sigma_p(i+1)$ is an edge in G for $1 \leqslant i < \ell$ and then $\sigma_p(i) = v_i$. A path $p = v_1 \to v_2 \to \cdots \to v_{\ell'}$ is *transitive*, if its transitive closure is a subgraph of G. In other words, p is transitive if $v_i \leftarrow v_j$ is an edge in G for all $1 \leqslant i < j \leqslant \ell 1$.

For a relation graph G on ℓ vertices with labels $d_1, d_2, \ldots, d_\ell$ and $n = \prod_{1 \leqslant i \leqslant \ell} d_i$, we define

$$\begin{aligned}\mathcal{D}_G = \{f \in \mathcal{P}_n :\ & \text{for every transitive Hamiltonian path} \\ & e_1 \leftarrow \cdots \leftarrow e_\ell \text{ in G, there are } g_i \in \mathcal{P}_{e_i} \text{ for } 1 \leqslant i \leqslant \ell \\ & \text{with } f = g_1 \circ g_2 \circ \cdots \circ g_\ell\}.\end{aligned}$$

If $G = \{d\}$ is a singleton, we have $\mathcal{D}_G = \mathcal{P}_d$. If $G = d \to e$, we have $\mathcal{D}_G = \mathcal{P}_d \circ \mathcal{P}_e$.

Proposition 3.3.2. *Let* n *be a positive integer,* D *a normalized set of ordered factorizations of* n*, and* G *the relation graph of* D*. We have*

$$\mathcal{D}_{n,D} = \mathcal{D}_G.$$

Proof. Every transitive tournament G_d for $d \in D$, has d as its unique transitive Hamiltonian path. Since G is the union of all such G_d, we have "$\supseteq$".

For "$\subseteq$", we have to show that every polynomial with decomposition degree sequences D also has decomposition degree sequence d^* for every transitive Hamiltonian path d^* in G. We proceed on two levels. First, we derive all transitive Hamiltonian paths in G from "twisting" the paths given by D. Second, we show that the corresponding "twisted" decomposition degree sequences follow from the given ones.

Let d^* be a transitive Hamiltonian path in G and $d \in D$ arbitrary. We use Bubble-Sort to transform d into d^* and call the intermediate states after k passes $d^{(k)}$, $0 \leqslant k \leqslant c$, such that $d^{(0)} = d$ and $d^{(c)} = d^*$.

Algorithm 3.3.3: Bubble-Sort d according to d^*

```
1  ℓ ← |d|
2  k ← 0, d^(0) ← d
3  while d^(k) ≠ d* do
4  |  k ← k + 1, d^(k) ← d^(k−1)        /* copy previous state */
5  |  for i = 1, ..., ℓ − 1 do
6  |  |  σ = σ(d^(k), d*)
7  |  |  if σ(i) > σ(i + 1) then
8  |  |  |  (d_i^(k), d_{i+1}^(k)) ← (d_{i+1}^(k), d_i^(k))        /* swap */
9  |  |  end
10 |  end
11 end
12 c ← k
```

In other words, $d^{(k)}$ is obtained from $d^{(k-1)}$ by at most $\ell - 1$ "swaps" of adjacent vertices. Figure 3.3.4 visualizes a swap of $d_i^{(k)}$ and $d_{i+1}^{(k)}$ as in step 8. The fundamental properties of Bubble-Sort guarantee correctness and $c \leqslant \ell(\ell-1)/2$, see Cormen, Leiserson, Rivest & Stein (2009, Problem 2.2).

Furthermore, the following holds.

(i) Every pair $(d_i^{(k)}, d_{i+1}^{(k)})$ of swapped vertices in step 8 is connected by a bidirectional edge in G.

(ii) Every $d^{(k)}$, $0 \leqslant k \leqslant c$, is a transitive Hamiltonian path in G.

For (i), we have the edge $d_i^{(k)} \leftarrow d_{i+1}^{(k)}$ from $d^{(k-1)}$ and the edge $d^*_{\sigma(i+1)} = d_{i+1}^{(k)} \leftarrow d_i^{(k)} = d^*_{\sigma(i)}$ from d^* with σ as in step 6.

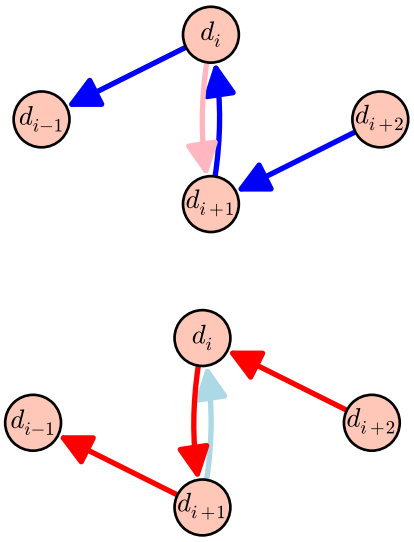

Figure 3.3.4: A "swap" between two transitive Hamiltonian paths $d_{i-1} \leftarrow d_i \leftarrow d_{i+1} \leftarrow d_{i+2}$ and $d_{i-1} \leftarrow d_i \leftarrow d_{i+1} \leftarrow d_{i+2}$ along the bidirectional edge between d_i and d_{i+1}.

For $k = 0$, (ii) holds by definition. For $k > 0$ it follows inductively from $k-1$, since a swap merely replaces the 4-subpath $d_{i-1} \leftarrow d_i \leftarrow d_{i+1} \leftarrow d_{i+2}$ by $d_{i-1} \leftarrow d_{i+1} \leftarrow d_i \leftarrow d_{i+2}$, where the outer edges are guaranteed in G by transitivity of $d^{(k-1)}$ and the inner edge by (i). Thus, the swapped path is also a transitive Hamiltonian path in G.

Now, we mirror the "swaps" of vertices by "Ritt moves" of components as introduced by Zieve & Müller (2008).

Claim 3.3.5 (Ritt moves). *Let* $g_1 \circ \cdots \circ g_\ell = h_1 \circ \cdots \circ h_\ell$ *be decompositions with degree sequence* d *and* e*, respectively. Let* d *and* e *be aligned,* $\sigma = \sigma(\mathsf{d}, \mathsf{e})$*, and* $1 \leqslant i < \ell$ *with* $\sigma(i) > \sigma(i+1)$*. Then*

$$g_i \circ g_{i+1} = g_i^* \circ g_{i+1}^*$$

with $\deg(g_i) = \deg(g_{i+1}^*)$ *and* $\deg(g_{i+1}) = \deg(g_i^*)$*. Therefore, if some monic original polynomial* f *has decomposition degree sequences* d *and* e*, it also has the decomposition degree sequence* $\mathsf{d}^* = (d_1, \ldots, d_{i-1}, d_{i+1}, d_i, d_{i+2}, \ldots, d_\ell)$.

The claim is based on the following lemma.

Lemma 3.3.6. *Let* d *and* e *be aligned ordered factorizations,* $\sigma = \sigma(\mathsf{d}, \mathsf{e})$*,* $1 \leqslant i \leqslant |\mathsf{d}|$*, and* $j = \sigma(i)$*. Then*

$$\begin{aligned}\gcd(&d_1 \cdot \ldots \cdot d_{i-1}, e_1 \cdot \ldots \cdot e_{j-1}) \\ &= \gcd(d_1 \cdot \ldots \cdot d_{i-1} \cdot d_i, e_1 \cdot \ldots \cdot e_{j-1})\end{aligned}$$

$$= \gcd(d_1 \cdot \ldots \cdot d_{i-1}, e_1 \cdot \ldots \cdot e_{j-1} \cdot e_j).$$

In particular, (3.2.7) *holds.*

Proof of lemma. For any $1 \leqslant k < j$, with $\gcd(e_k, e_j) = \gcd(e_k, d_i) > 1$, we have $\sigma^{-1}(k) < i$ due to (3.2.4). In other words, σ^{-1} maps all indices $1 \leqslant k < j$, where $\gcd(e_k, d_i) > 1$, into the set $\{1, \ldots, i-1\}$. Therefore

$$\gcd\Big(\frac{e_1 \cdot \ldots \cdot e_{j-1}}{\gcd(d_1 \cdot \ldots \cdot d_{i-1}, e_1 \cdot \ldots \cdot e_{j-1})}, d_i\Big) = 1,$$

$$\begin{aligned}
&\gcd(d_1 \cdot \ldots \cdot d_{i-1} \cdot d_i, e_1 \cdot \ldots \cdot e_{j-1}) \\
&\quad = \gcd(\gcd(d_1 \cdot \ldots \cdot d_{i-1}, e_1 \cdot \ldots \cdot e_{j-1}) d_i, e_1 \cdot \ldots \cdot e_{j-1}) \\
&\qquad = \gcd(d_1 \cdot \ldots \cdot d_{i-1}, e_1 \cdot \ldots \cdot e_{j-1}). \quad \square
\end{aligned}$$

Let $j' = \sigma(i+1) < \sigma(i) = j$, $A = g_1 \circ \cdots \circ g_{i-1}$, $C = g_{i+2} \circ \cdots \circ g_\ell$, $A' = h_1 \circ \cdots \circ h_{j'-1}$, $B' = h_{j'+1} \circ \cdots \circ h_{j-1}$, and $C' = h_{j+1} \circ \cdots \circ h_\ell$, such that

$$A \circ g_i \circ g_{i+1} \circ C = A' \circ h_{j'} \circ B' \circ h_j \circ C'.$$

Lemma 3.3.6 for i and $i+1$ yields

$$\gcd(\deg(A \circ g_i), \deg(A' \circ h_{j'} \circ B')) = \gcd(\deg(A), \deg(A' \circ h_{j'} \circ B')),$$

$$\gcd(\deg(A \circ g_i \circ g_{i+1}), \deg(A')) = \gcd(\deg(A \circ g_i), \deg(A' \circ h_{j'})),$$

respectively. From the former, we derive

$$\begin{aligned}
1 &= \gcd\Big(g_i, \frac{\deg(A' \circ h_{j'} \circ B')}{\gcd(\deg(A), \deg(A' \circ h_{j'} \circ B'))}\Big) \\
&= \gcd\Big(g_i, \frac{\deg(A' \circ h_j)}{\gcd(\deg(A), \deg(A' \circ h_{j'}))}\Big).
\end{aligned}$$

And then continue the latter as

$$\begin{aligned}
&\gcd(\deg(A \circ g_i \circ g_{i+1}), \deg(A')) \\
&= \gcd(\deg(A \circ g_i), \deg(A' \circ h_{j'})) \\
&= \gcd(\deg(A), \deg(A' \circ h_{j'})) \cdot \gcd\Big(g_i, \frac{\deg(A' \circ h_{j'})}{\gcd(\deg(A), \deg(A' \circ h_{j'}))}\Big) \\
&= \gcd(\deg(A), \deg(A' \circ h_{j'})). \qquad (3.3.7)
\end{aligned}$$

Let $G = g_i \circ g_{i+1}$ and $H = h_j$. We have $\gcd(d_i, d_{i+1}) = 1$ due to the "twisting condition" $\sigma(i+1) < \sigma(i)$ and thus $\gcd(\deg(G), \deg(H)) = d_{i+1}$. We apply Lemma 3.2.6 with $g_i = G$, $h_j = H$, and $c = d_{i+1}$ in

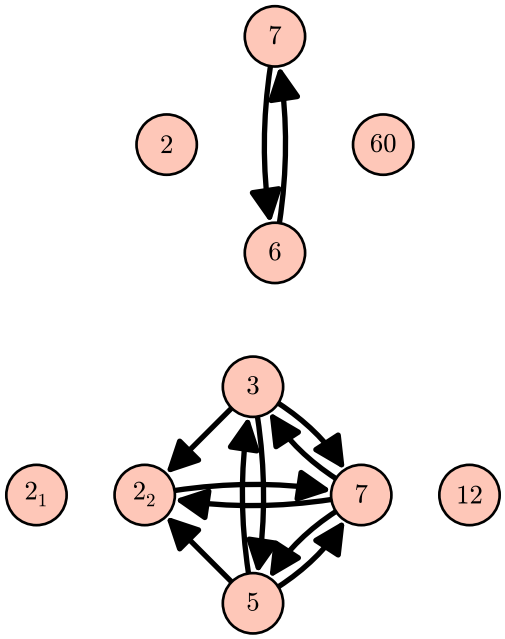

Figure 3.4.1: The three strongly connected components of each relation graph in Figure 3.3.1, respectively.

the notation of that claim, and find, since (3.3.7) provides condition (3.2.7),

$$G = g_i^* \circ g_{i+1}^*$$

with $\deg(g_i^*) = d_{i+1}$ and $\deg(g_{i+1}^*) = d_i$ as required.

Repeated application of Claim 3.3.5 shows that for every $f \in \mathcal{D}_{n,D}$, $d \in D$, and every transitive Hamiltonian path d^* in G, we have $d^{(k)}$ as in Algorithm 3.3.3 as decomposition degree sequence. In particular, $d^{(c)} = d^*$. □

3.4 STRUCTURE AND SIZE OF $\mathcal{D}_{n,D}$

Measure what is measurable,
and make measurable what is not so.
— Galileo Galilei

Every directed graph admits a decomposition into strictly connected components, where any two distinct vertices are connected by paths in either direction. Since a relation graph G is the union of directed complete graphs, its strictly connected components G_i, $1 \leqslant i \leqslant \ell$, are again relation graphs and form a chain $G_1 \leftarrow G_2 \leftarrow \cdots \leftarrow G_\ell$. Figure 3.4.1 shows the connected components of the relation graphs Figure 3.3.1

Theorem 3.4.2. *Let n be coprime to the characteristic of F, D a nonempty set of ordered factorizations of n, and G the relation graph of D with strongly connected components $G_1 \leftarrow G_2 \leftarrow \cdots \leftarrow G_\ell$. Then the composition map*

$$\prod_{1 \leqslant i \leqslant \ell} \mathcal{D}_{G_i} \to \mathcal{D}_G, \quad (g_i)_{1 \leqslant i \leqslant \ell} \mapsto g_1 \circ g_2 \circ \dots g_\ell \tag{3.4.3}$$

is bijective. Thus,

$$\mathcal{D}_G = \mathcal{D}_{G_1} \circ \mathcal{D}_{G_2} \circ \cdots \circ \mathcal{D}_{G_\ell}$$

and over a finite field $F = \mathbb{F}_q$ with q elements, we have

$$\#\mathcal{D}_G = \prod_{1 \leqslant i \leqslant \ell} \#\mathcal{D}_{G_i}.$$

Proof. The map (3.4.3) is injective due to the absence of equal-degree collisions. To show that it is surjective, we show that for any $f \in \mathcal{D}_G$, we have uniquely determined $g_i \in \mathcal{D}_{G_i}$ such that $f = g_1 \circ g_2 \circ \cdots \circ g_\ell$ and for any tuple $(g_i) \in \prod$.

For $f \in \mathcal{P}_n$, where $n = \prod_{v \in G} v$, we show that the following are equivalent.

(i) The polynomial f has decomposition degree sequence d for every transitive Hamiltonian path d in G.

(ii) The polynomial f has decomposition degree sequence $d = d_1 \leftarrow d_2 \leftarrow \cdots \leftarrow d_\ell$ for every concatenation of transitive Hamiltonian paths d_i in G_i for $1 \leqslant i \leqslant \ell$.

Assume (i) and let $d = d_1 \leftarrow d_2 \leftarrow \cdots \leftarrow d_\ell$ be the concatenation of transitive Hamiltonian paths d_i in G_i for $1 \leqslant i \leqslant \ell$ as in (ii). Then d_i is a Hamiltonian path in G. Since the underlying undirected graph of G is complete, we have $d_i \leftarrow d_j$ in G for any vertices $d_i \in G_i$ and $d_j \in G_j$ in distinct strictly connected components with $i < j$. Thus d is also transitive and f has decomposition degree sequence d by (i).

Conversely, assume (ii) and observe that the decomposition of G into strictly connected components induces a decomposition of every transitive Hamiltonian path d in G into Hamiltonian paths d_i in G_i. These are transitive, since transitivity is a local condition and f has decomposition degree sequence d by (ii).

Uniqueness and thus the counting formula follow from the absence of equal-degree collisions in the tame case. □

We split the edge set E of a strictly connected relation graph G with vertices V into its uni-directional edges $\overrightarrow{E} = \{(u, v) \in E : (v, u) \notin E\}$ and its bi-directional edges (2-loops) $\overline{E} = \{\{u, v\} \subseteq V : \{(u, v), (v, u)\} \in E\} = E \setminus \overrightarrow{E}$. We call the corresponding graphs on V the *directed* and the *undirected* subgraph of G, respectively. The directed subgraph of G is

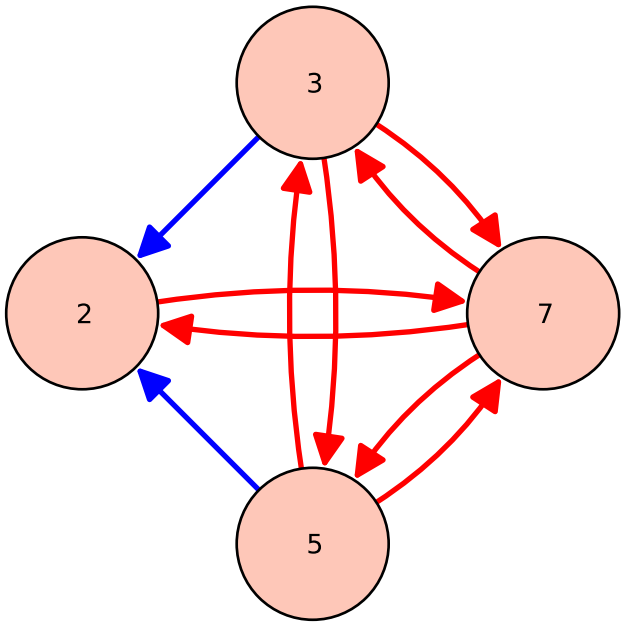

Figure 3.4.4: The strongly connected component on 4 vertices of Figure 3.4.1 decomposed into its undirected subgraph (red) and its directed subgraph (blue) with MAX-SINK-sorting $7 \prec 2 \prec 5 \prec 3$.

a *directed acyclic graph* since G is the union of transitive tournaments. The undirected subgraph of G is connected. It is also the union of the *permutation graphs* of σ_k, $1 \leqslant k \leqslant c$.

The directed subgraph $\overrightarrow{G}$ captures the requirements on the position of the degrees in a decomposition sequence. The undirected subgraph $\overline{G}$ captures the admissible Ritt moves d'après Zieve & Müller (2008) and thus the requirements on the shape of the components.

Every directed acyclic graph admits a *topological sorting* $v_1, v_2, \ldots, v_\ell$ of its vertices, where a directed edge $v_i \leftarrow v_j$ in $\overrightarrow{G}$ implies $i < j$, see Cormen *et al.* (2009, Section 22.4) or (Knuth, 1973, Exercise 2.3.4.2.4). A directed acyclic graph may have several distinct topological sortings. Tarjan (1976) suggested to use DEPTH-FIRST-SEARCH on $\overrightarrow{G}$. The time step, when DEPTH-FIRST-SEARCH visits a vertex for the last time, is called the *finish time* of the vertex and listing the vertices with increasing finish time yields a topological sorting. The result is unique, if the tie-break rule in the expansion step of DEPTH-FIRST-SEARCH is deterministic. We use the following terminology.

Let $U(v)$ denote the open $\overline{G}$-neighborhood of a vertex v. It is always nonempty. We call a vertex v *locally maximal*, if its value is greater or equal than the value of every vertex in $U(v)$. Since vertices with equal values are never connected by an edge in $\overline{G}$, a locally maximal v is always strictly greater than all vertices in $U(v)$. Further-

more, there is at least one locally maximal vertex, namely a "globally" maximal one. There is a unique enumeration of the locally maximal vertices $d_1, d_2, \ldots, d_m$ such that

$$d_1 \leftarrow d_2 \leftarrow \cdots \leftarrow d_m$$

is a directed path in G. Furthermore, we define for $1 \leqslant i \leqslant m$,

$$\begin{aligned} V_i &= U(d_i) \setminus U(d_{i+1}) \text{ and } W_i = V_i \cup \{d_i\}, \\ V_0 &= W_0 = \{v \in G\colon \text{ no edge } d_i \leftarrow v \text{ in } G \text{ for any } 1 \leqslant i \leqslant m\}, \\ V_{m+1} &= W_{m+1} = \{v \in G\colon \text{ no edge } v \leftarrow d_i \text{ in } G \text{ for any } 1 \leqslant i \leqslant m\}. \end{aligned}$$

The W_i, $0 \leqslant i \leqslant m+1$, form a partition of all vertices of $\overrightarrow{G}$ and we formulate the tie-break rule for Depth-First-Search as follows. Given vertices $u \in W_i$ and $v \in W_j$ with $i < j$, the vertex u is preferred. Given vertices $u, v \in W_i$, the vertex with the larger value is preferred. Since vertices with equal value are always connected by a unidirectional edge in $\overrightarrow{G}$ due to (3.2.4), the search has never to choose between to vertices with the same value and Depth-First-Search with this tie-break rule yields a unique topological sorting. We call it the Max-Sink topological sorting of $\overrightarrow{G}$. Figure 3.4.4 shows the largest strongly connected component of Figure 3.4.1 and its Max-Sink topological sorting.

Theorem 3.4.5. *Let G be a strongly connected relation graph with at least two vertices, $\overrightarrow{G}$ its directed subgraph, and $\overline{G}$ its undirected subgraph. Let $d_1, d_2, \ldots, d_\ell$ be the* Max-Sink *topological sorting of $\overrightarrow{G}$ and let e_i be the product of all vertices in the open $\overline{G}$-neighborhood of d_i. For every $f \in \mathcal{D}_G$ either (i) or (ii) holds, and (iii) is also valid.*

(i) (Exponential Case) There are unique $g_i \in \mathcal{E}_{d_i}^{(e_i)}$ for $1 \leqslant i \leqslant \ell$ and $a \in F$ such that

$$f = (g_1 \circ g_2 \circ \cdots \circ g_\ell)^{[a]}.$$

(ii) (Trigonometric Case) There are unique $z, a \in F$ with $z \neq 0$ such that

$$f = T_{d_1 d_2 \cdots d_\ell}(x, z)^{[a]}.$$

(iii) If $\overline{G}$ contains no edge that connects two vertices both larger than 2, then the Trigonometric Case is included in the Exponential Case. Otherwise, they are mutually exclusive.

Furthermore,

$$\mathcal{D}_{n,G} = \mathcal{T}^{[F]}_{d_1 d_2 \cdots d_m} \cup (\mathcal{E}^{(e_1)}_{d_1} \circ \mathcal{E}^{(e_2)}_{d_2} \circ \cdots \circ \mathcal{E}^{(e_m)}_{d_m})^{[F]}. \tag{3.4.6}$$

The e_i are well-defined, since there are no empty neighborhoods in the connected graph $\overline{G}$ with at least two vertices.

Proof. We begin with the proof of existence, then show uniqueness and conclude with the "converse" (3.4.6).

The MAX-SINK topological sorting $d_1, d_2, \dots, d_\ell$ of $\overrightarrow{G}$ yields a transitive Hamiltonian path

$$d = d_1 \prec d_2 \prec \cdots \prec d_\ell$$

in G. For the rest of the proof, we identify the MAX-SINK topological sorting with the corresponding transitive Hamiltonian path.

We (re)label the locally maximally vertices $d_1, d_2, \dots, d_m$ and the elements of V_i as $d_i^{(1)}, d_i^{(2)}, \dots, d_i^{(\ell_i)}$ for $0 \leqslant i \leqslant m+1$ and $\ell_i = \#V_i$ such that

$$\begin{aligned} d &= (d_0^{(1)}, \dots, d_0^{(\ell_0)}, d_1, d_1^{(1)}, \dots, d_1^{(\ell_1)}, d_2, d_2^{(1)}, \dots, \\ &\quad d_{m-1}^{(\ell_{m-1})}, d_m, d_m^{(1)}, \dots, d_m^{(\ell_m)}, d_{m+1}^{(1)}, \dots, d_{m+1}^{(\ell_{m+1})}) \\ &= (V_0, d_1, V_1, d_2, \dots, d_m, V_m, V_{m+1}), \end{aligned}$$

where the V_i are read as tuple $(d_i^{(1)}, d_i^{(2)}, \dots, d_i^{(\ell_i)})$. Then f has a decomposition

$$\begin{aligned} f = G_0^{(1)} \circ \cdots \circ G_0^{(\ell_0)} \circ G_1 \circ G_1^{(1)} \circ \cdots \circ G_1^{(\ell_1)} \circ G_2 \circ G_2^{(1)} \circ \dots \\ \circ G_{m-1}^{(\ell_{m-1})} \circ G_m \circ G_m^{(1)} \circ \cdots \circ G_m^{(\ell_m)} \circ G_{m+1}^{(1)} \circ \cdots \circ G_{m+1}^{(\ell_{m+1})} \end{aligned} \tag{3.4.7}$$

with $G_i^{(j)} \in \mathcal{P}_{d_i^{(j)}}$ for $0 \leqslant i \leqslant m+1$, $1 \leqslant j \leqslant \ell_i$, and $G_i \in \mathcal{P}_{d_i}$ for $1 \leqslant i \leqslant m$.

We assume for the moment that all edges in $\overline{G}$ contain a 2. Then Theorem 3.1.10 reduces to the exponential case, and we proceed as follows. First, we show that every $G_i^{(j)}$ for $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant \ell_i$, is of the form $g_i^{[a_i]}$ for unique $g_i \in \mathcal{E}_{d_i^{(j)}}^{(e_i^{(j)})}$ and unique $a_i \in F$. Then, we extend this to $i = 0$ and $i = m+1$. Finally, we show that the shifting parameters a_i are "compatible" such that a single shifting parameter a suffices.

For every $1 \leqslant i \leqslant m$, we use BUBBLE-SORT Algorithm 3.3.3 with Lemma 3.4.8 to obtain the decomposition degree sequence

$$(V_0, d_1, V_1, \dots, d_i, V_i, d_i^{(\ell_{i+1})}, \dots d_i^{(m_i)}, d_{i+1}, \hat{V}_{i+1}, \dots, d_m, \hat{V}_m, V_{m+1}),$$

where $U(d_i) = V_i \cup \{d_i^{(\ell_{i+1})}, \dots d_i^{(m_i)}\}$ and the latter elements have been omitted from $V_{i+1}, \dots, V_m$. We have $e_i = \prod_{1 \leqslant j \leqslant m_i} d_i^{(j)}$ and this implies the two decomposition degree sequences

$$\begin{aligned} &(V_0, d_1, V_1, \dots, d_i, e_i, d_{i+1}, \hat{V}_{i+1}, \dots, d_m, \hat{V}_m, V_{m+1}), \\ &(V_0, d_1, V_1, \dots, e_i, d_i, d_{i+1}, \hat{V}_{i+1}, \dots, d_m, \hat{V}_m, V_{m+1}). \end{aligned}$$

Thus, there are unique $g_i \in \mathcal{E}_{d_i}^{(e_i)}$ and $a_i \in F$ such that in (3.4.7), we have

$$G_i \circ G_i^{(1)} \circ \cdots \circ G_i^{(\ell_i)} = (g_i \circ x^{d_i^{(1)}} \circ \cdots \circ x^{(d_i^{(\ell_i)})})^{[a_i]}.$$

The same form applies to $i = 0$, since there is at least one $d_i^{(j)}$ with $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant \ell_i$ that is in the $\overline{G}$-neighborhood of some element of V_0 due to the strong connectedness of G. And since there is no locally maximal element in V_0 all components are of the form $x^{d_0^{(j)}}$ with possible some shift applied. Every connection in G relates the corresponding shifting parameters and since G has a Hamiltonian path, they are all determined by a single choice.

Now to the general case, where some collisions may be trigonometric, but not exponential. For any two locally maximal vertices d_i and d_j there is some vertex $d \in U(d_i) \cap U(d_j)$. This shows that either all blocks fall into the exponential case or all blocks fall into the trigonometric case. The two cases are disjoint if and only if there is some edge in $\overline{G}$ that connects two vertices both with value greater than 2.

The stabilizer of original shifting is $\{0\}$ for nonlinear monic original polynomials and there are no equal-degree collisions. Hence the representation is unique.

The converse (3.4.6) is a direct computation. □

Lemma 3.4.8. *Let $i < j$ and d_j in the open $\overline{G}$-neighborhood of d_i. Then for every $i < k < j$, we have d_k in the open $\overline{G}$-neighborhood of d_i or d_j or both.*

Proof. The tournaments underlying G are acyclic. Therefore, if $d_i \prec d_k \prec d_j$ and $d_j \prec d_k$, then at least one other edge is bidirectional, too. □

The classification of Theorem 3.4.5 yields the exact number of decomposable polynomials of degree n over a finite field $\mathbb{F}_q$.

Theorem 3.4.9. *Let G be a strongly connected relation graph of n with undirected subgraph $\overline{G}$. Let $d_1, d_2, \ldots, d_\ell$ be the vertices of $\overline{G}$ and e_i be the product of all vertices in the (open) $\overline{G}$-neighborhood of d_i. Let $\delta_{\overline{G},2}$ be 1 if there is no edge in $\overline{G}$ between two vertices both larger than 2 and let $\delta_{\overline{G},2}$ be 0 otherwise. Then*

$$\#\mathcal{D}_G = \begin{cases} q^{d-1} & \text{if } G = \{d\}, \\ q \cdot (\prod_{d_i \in G} q^{\lfloor d_i/e_i \rfloor} + (1 - \delta_{\overline{G},2}) \cdot (q-1)) & \text{otherwise.} \end{cases}$$

Proof. For $G = \{d\}$, this follows from (3.1.3). Otherwise from the (non)uniqueness of the parameters in Theorem 3.4.5. □

We are finally ready to employ the inclusion-exclusion formula (3.1.6) from the beginning. For a nonempty set D of nontrivial divisors of n, it requires $\#\mathcal{D}_{n,D} = \#\mathcal{D}_{n,D}$ for $D = \{(d, n/d) \colon d \in D\}$.

We compute a normalization D^* by repeated application of Algorithm 3.2.18 and derive the relation graph of D^*. Then $\#\mathcal{D}_{n,D} = \#\mathcal{D}_G$ and the latter follows from Theorem 3.4.2 and Theorem 3.4.9.

Algorithm 3.4.10: Count decomposables

Input: positive integer n
Output: $\#\mathcal{D}_n(\mathbb{F}_q)$ as a polynomial in q for n coprime to q

if $n = 1$ *or* n *is prime* **then**
  return 0
end
total $\leftarrow 0$
$N \leftarrow \{1 < d < n : d \mid n\}$
for $\varnothing \neq D \subseteq N$ **do**
  $D \leftarrow \{(d, n/d) : d \in D\}$
  $D^* \leftarrow$ normalization of D
  $G \leftarrow$ relation graph of D^*
  collisions $\leftarrow 1$
  for *strongly connected components* G_j *of* G **do**
    $\overline{G}_j \leftarrow$ undirected subgraph of G_j
    if $G_j = \{d\}$ **then**
      connected $\leftarrow q^{d-1}$
    else
      $\{d_1, d_2, \ldots, d_\ell\} \leftarrow G_j$
      for $i = 1, \ldots, \ell$ **do**
        $U_i \leftarrow$ open neighborhood of d_i in $\overline{G}_j$
        $e_i \leftarrow \prod_{v \in U_i} v_i$
      end
      connected $\leftarrow \prod_{d_i \in G_j} q^{\lfloor d_i/e_i \rfloor}$
      if *some edge in* $\overline{G}_j$ *connects two vertices both larger than 2* **then**
        connected $\leftarrow$ connected $+ q - 1$
      end
      connected $\leftarrow$ connected $\cdot\, q$
    end
    collisions $\leftarrow$ collisions $\cdot$ connected
  end
  total $\leftarrow$ total $+ (-1)^{\#D} \cdot$ collisions
end
return total

This is easy to implement, see Algorithm 3.4.10, and yields the exact expressions for $\#\mathcal{D}_n(\mathbb{F}_q)$ at lightning speed, see Table 3.4.11. The expressions fit within the bounds given by von zur Gathen (2014a, Theorem 3.2) and match the explicit formulas in the cited work for composite n with one or two nontrivial divisors.

Let ℓ be the smallest prime divisor of n and τ the number of positive divisors of n. The naive method for counting the number of decomposables at degree n loops over all $\tau - 2$ nontrivial divisors d of n, computes the composition of all $\mathcal{P}_d \times \mathcal{P}_{n/d}$, and stores them in a sorted list to catch duplicates. This requires $O(q^{\ell+n/\ell-2})$ memory and $O(\tau q^{\ell+n/\ell-2})$ compositions of polynomials of degree at most n/ℓ.

General bounds on τ are $\tau \geqslant 3$, if n is composite, and $\limsup(\ln \tau \ln\ln n / \ln n) = \ln 2$ by Wigert (1907), so that $\tau = O(n^{1/(\operatorname{loglog} n)})$, see Hardy & Wright (1985, Theorem 317), For the average as $n \to \infty$, Dirichlet provides $x^{-1} \sum_{n \leqslant x} \tau(n) = \ln x + 2\gamma - 1 + O(x^{\theta-1/2})$, where γ is Euler's constant, see Apostol (1976, Theorem 3.3). Improving the error term is known as *Dirichlet's divisor problem* and the most recent value is $\theta = 131/416 \approx 0.31490$ by Huxley (2003).

Algorithm 3.4.10 requires $2^{\tau-2} - 1$ evaluations of the collision counting formula and stores at most n integer coefficients. More importantly it requires only integer and graph operations, independent from q, while the naive method requires field operations and therefore depends on q.

3.5 CONCLUSION AND FUTURE WORK

> As long as a branch of science offers an abundance of problems, so long it is alive; a lack of problems foreshadows extinction or the cessation of independent development.
>
> — David Hilbert

We presented a normal form for multi-collisions of decompositions of arbitrary length with exact description of the (non)uniqueness of the parameters. This led to an exact formula for the number of such collisions of degree n over a finite field of characteristic coprime to n. We concluded with a fast algorithm to compute the exact number of decomposable polynomials of degree n over a finite field $\mathbb{F}_q$ in the tame case.

We introduced the relation graph of a set of collisions which is related to transitive tournaments and permutation graphs. The relation graph of a single polynomial may be of independent interest as a data structure. Furthermore, it would be useful to characterize sets D of ordered factorizations that lead to identical contributions $\#\mathcal{D}_{n,D}$ and to quickly derive $\#\mathcal{D}_{n,D\cup\{e\}}$ from $\#\mathcal{D}_{n,D}$ or conversely. Finally, this chapter deals with polynomials only and the study of rational functions with the same methods remains open. Here, Gutierrez & Sevilla (2006a) provide counterexamples to generalizations of Ritt's First Theorem to rational functions.

n	$\#D_n(\mathbb{F}_q)$	lower bound, upper bound
4	q^2	
6	$2q^3-q^2$	
8	$2q^4-q^3$	
9	q^4	
10	$2q^5-q^3$	
12	$2q^6+2q^5-3q^4-q^2+q$	$2q^6-q^4, 2q^6-q^4-\frac{2q^5}{\frac{1}{q}-1}$
14	$2q^7-q^4$	
15	$2q^6-2q^2+q$	
16	$2q^8+q^6-3q^5+q^4$	$2q^8-q^5, 2q^8-q^5-\frac{2q^6}{\frac{1}{q}-1}$
18	$2q^9+2q^7-4q^5+q^3$	$2q^9-2q^5, 2q^9-\frac{2q^7}{\frac{1}{q}-1}-q^5$
20	$2q^{10}+2q^7-3q^6$	$2q^{10}-q^6, 2q^{10}-q^6-\frac{2q^7}{\frac{1}{q}-1}$
21	$2q^8-q^3-q^2+q$	
22	$2q^{11}-q^6$	
24	$2q^{12}+2q^9+2q^8-3q^7-6q^6+4q^5-q^3+2q^2-q$	$2q^{12}-q^7, 2q^{12}-\frac{2q^9}{\frac{1}{q}-1}-q^7$
25	q^8	
26	$2q^{13}-q^7$	
27	$2q^{10}-q^6$	
28	$2q^{14}+2q^9-3q^8$	$2q^{14}-q^8, 2q^{14}-q^8-\frac{2q^9}{\frac{1}{q}-1}$
30	$2q^{15}+2q^{11}+2q^9-q^8-6q^7+q^4+q^2$	$2q^{15}-2q^8, 2q^{15}-\frac{2q^{11}}{\frac{1}{q}-1}-q^8$
32	$2q^{16}+2q^{10}-3q^9-3q^7+4q^6-q^5$	$2q^{16}-q^9, 2q^{16}-q^9-\frac{2q^{10}}{\frac{1}{q}-1}$
33	$2q^{12}-q^4-q^2+q$	
34	$2q^{17}-q^9$	
35	$2q^{10}-2q^2+q$	
36	$2q^{18}+2q^{13}+2q^{11}-2q^{10}-6q^8-3q^7+6q^6$	$2q^{18}-q^{10}, 2q^{18}-\frac{2q^{13}}{\frac{1}{q}-1}-q^{10}$
38	$2q^{19}-q^{10}$	
39	$2q^{14}-q^5-q^2+q$	
40	$2q^{20}+2q^{12}-q^{11}-6q^8+4q^7-q^2+q$	$2q^{20}-q^{11}, 2q^{20}-q^{11}-\frac{2q^{12}}{\frac{1}{q}-1}$
42	$2q^{21}+2q^{15}+q^{11}-6q^9+q^5+2q^3-q^2$	$2q^{21}-2q^{11}, 2q^{21}-\frac{2q^{15}}{\frac{1}{q}-1}-q^{11}$
44	$2q^{22}+2q^{13}-3q^{12}$	$2q^{22}-q^{12}, 2q^{22}-q^{12}-\frac{2q^{13}}{\frac{1}{q}-1}$
45	$2q^{16}+2q^{12}-3q^8-q^2+q$	$2q^{16}-q^8, 2q^{16}-\frac{2q^{12}}{\frac{1}{q}-1}-q^8$
46	$2q^{23}-q^{12}$	
48	$2q^{24}+2q^{17}+2q^{14}-3q^{13}+2q^{12}-6q^{10}-6q^9+q^8+12q^7-6q^6+3q^3-3q^2+q$	$2q^{24}-q^{13}, 2q^{24}-\frac{2q^{17}}{\frac{1}{q}-1}-q^{13}$
49	q^{12}	
50	$2q^{25}+q^{13}-3q^9+q^5$	$2q^{25}-2q^{13}, 2q^{25}-q^{13}-\frac{2q^{13}}{\frac{1}{q}-1}$

Table 3.4.11: Exact values of $\#\mathcal{D}_n(\mathbb{F}_q)$ in the tame case for composite $n \leqslant 50$, consistent with the upper and lower bounds (in the last column) or exact values (no entry in the last column) of von zur Gathen (2014a, Theorem 3.2). The computation took 8.53 s (average over 100 trials) with `Sage` using a single core 2.4 GHz CPU and 4 GB RAM.

4

COUNTING DECOMPOSABLE POLYNOMIALS: THE WILD CASE

> The creator of the new composition [...]
> is an outlaw until he is a classic.
> — Gertrude Stein

An earlier version of this chapter appeared as Blankertz, von zur Gathen & Ziegler (2013)[1], see Section 1.3 for the complete publication history.

In this chapter, we study only *equal-degree* collisions of $f = g \circ h = g^* \circ h^*$, where $\deg g = \deg g^*$ and thus $\deg h = \deg h^*$. The main result (Theorem 4.5.6) determines exactly the number of decomposable polynomials in one of open difficult cases, namely when $n = p^2$ and hence $\deg g = \deg h = p$.

This is shown in three steps. First, we exhibit some classes of collisions in Section 4.2. Their properties are easy to check. In the second step we show that these are all possibilities (Theorem 4.4.9). In Section 4.3 we use ramification theory of function fields to study the root multiplicities in collisions, and in Section 4.4 classify all collisions at degree p^2. In the third step we count the resulting possibilities (Section 4.5). We conclude with open questions and suggestions for future work in Section 4.6.

Our contribution is fourfold.

- We provide explicit constructions for collisions at degree r^2, where r is a power of the characteristic $p > 0$ (Fact 4.2.1, Theorem 4.2.22).
- We provide a classification of all collisions at degree p^2, linking every collision to a unique explicit construction (Theorem 4.4.9).
- We use these two results to obtain an exact formula for the number of decomposable polynomials at degree p^2 (Theorem 4.5.6).

[1] Notice: this is the authors' version of a work that was accepted for publication in *Journal of Symbolic Computation*. Changes resulting from the publishing process, such as peer review, editing, corrections, structural formatting, and other quality control mechanisms may not be reflected in this document. Changes have been made to this work since it was submitted for publication. A definitive version was subsequently published as Blankertz, von zur Gathen & Ziegler (2013).

- The classification yields an efficient algorithm to test whether a given polynomial of degree p^2 has a collision or not (Algorithm 4.4.14).

4.1 DEFINITIONS AND EXAMPLES

> If one should try to define algebra, it might be said that algebra deals with the formal combinations of symbols according to prescribed rules.
>
> — Oystein Ore

We consider a field F of positive characteristic $p > 0$. Composition of g and h with linear polynomials introduces inessential ambiguities in decompositions $f = g \circ h$. To avoid them, we normalize f, g, and h to be *monic original*, that is with leading coefficient 1 and constant coefficient 0 (so that the graph of f passes through the origin); see von zur Gathen (2014a).

For a nonnegative integer k, an (equal-degree) k-*collision* at degree n is a set of k distinct pairs (g, h) of monic original polynomials in $F[x]$ of degree at least 2, all with the same composition $f = g \circ h$ of degree n and $\deg g$ the same for all (g, h). A k-collision is called *maximal* if it is not contained in a $(k+1)$-collision. We also say that f has a (maximal) k-collision. Furthermore, g is a *left component* and h a *right component* of f. For $n \geqslant 1$, we define

$$\begin{aligned} P_n(F) &= \{f \in F[x] \colon f \text{ is monic original of degree } n\}, \\ D_n(F) &= \{f \in P_n(F) \colon f \text{ is decomposable}\}, \\ C_{n,k}(F) &= \{f \in P_n(F) \colon f \text{ has a maximal } k\text{-collision}\}. \end{aligned} \tag{4.1.1}$$

Thus $\#P_n(\mathbb{F}_q) = q^{n-1}$. We sometimes leave out F from the notation when it is clear from the context.

Let $f \in P_n$ have a k-collision C, $f' \neq 0$, and m be a divisor of n. If all right components in C are of degree m and indecomposable, then $k \leqslant (n-1)/(m-1)$; see Blankertz (2011, Corollary 3.27). For $n = p^2$, both components are of degree p and thus indecomposable and we find $k \leqslant p+1$; see also von zur Gathen, Giesbrecht & Ziegler (2010, Proposition 6.5 (iv)). For counting all decomposable polynomials of degree p^2 over $\mathbb{F}_q$, it is sufficient to count the sets $C_{p^2,k}$ of polynomials with maximal k-collision for $k \geqslant 2$, since

$$\#D_{p^2} = q^{2p-2} - \sum_{k \geqslant 2} (k-1) \cdot \#C_{p^2,k}. \tag{4.1.2}$$

Lemma 4.1.3. *In a decomposition (g, h), g is uniquely determined by $g \circ h$ and h.*

Proof. Let $f = g \circ h$. Consider the F-algebra homomorphism $\varphi \colon F[x] \to F[x]$ with $x \mapsto h$. Its kernel is trivial, since h is nonconstant, and thus

φ is injective. Hence there is exactly one $u \in F[x]$ such that $\varphi(u) = f$, namely $u = g$. □

Furthermore, g is easy to compute from $g \circ h$ and h by the generalized Taylor expansion; see von zur Gathen (1990a, Section 2). The following is a simple example of a collision.

Example 4.1.4. Let $r = p^e$. For $h \in P_r(F)$, we have

$$x^r \circ h = \varphi_r(h) \circ x^r, \tag{4.1.5}$$

where φ_r is the eth power of the *Frobenius endomorphism* on F, extended to polynomials coefficientwise. For $h \neq x^r$, we have a 2-collision $\{(x^r, h), (\varphi_r(h), x^r)\}$ and call it a *Frobenius collision*.

In the case $r = p$, we have the following description.

Lemma 4.1.6. *(i) Assume that $f \in P_{p^2}(F)$ has a 2-collision. Then it is a Frobenius collision if and only if $f' = 0$.*

(ii) A Frobenius collision of degree p^2 is a maximal 2-collision.

Proof. (i) If f is a Frobenius collision, then $f' = 0$ by definition. Conversely, let $f \in P_{p^2}(F)$ with $f' = 0$. Then $f \in F[x^p]$ and thus $f = g \circ x^p$ for some monic original polynomial g. Let $f = g^* \circ h^*$ be another decomposition of f. By Lemma 4.1.3, f and h^* determine g^* uniquely, hence $h^* \neq x^p$ and $h^{*\prime} \neq 0$. Thus from $f' = g^{*\prime}(h^*) \cdot h^{*\prime} = 0$ follows $g^{*\prime} = 0$ and hence $g^* = x^p$. Furthermore, $f = x^p \circ h^* = \varphi_p(h^*) \circ x^p$ by (4.1.5), $g = \varphi_p(h^*)$ by the uniqueness in Lemma 4.1.3, and f is a Frobenius collision.

(ii) Let $f = x^p \circ h = \varphi_p(h) \circ x^p$, with $h \neq x^p$, be a Frobenius collision, and (g^*, h^*) a decomposition of f. Then $0 = f' = g^{*\prime}(h^*) \cdot h^{*\prime}$ and thus $g^{*\prime} = 0$ or $h^{*\prime} = 0$. If $h^{*\prime} = 0$, then $h^* = x^p$ and thus $g^* = \varphi_p(h)$, by Lemma 4.1.3. If $g^{*\prime} = 0$, then $g^* = x^p$ and $f = \varphi_p(h^*) \circ x^p$ as in (i). Thus $\varphi_p(h^*) = \varphi_p(h)$ by the uniqueness in Lemma 4.1.3, which implies $h = h^*$. □

If F is perfect—in particular if F is finite or algebraically closed—then the Frobenius endomorphism φ_p is an automorphism on F. Thus for $f \in P_{p^2}(\mathbb{F}_q)$, $f' = 0$ implies that f is either a Frobenius collision or x^{p^2}.

For $f \in P_n(F)$ and $w \in F$, the *original shift* of f by w is

$$f^{[w]} = (x - f(w)) \circ f \circ (x + w) \in P_n(F).$$

We also simply speak of a *shift*. Original shifting defines a group action of the additive group of F on $P_n(F)$. Indeed, we have for $w, w' \in F$

$$\begin{aligned}(f^{[w]})^{[w']} &= (x - f^{[w]}(w')) \circ f^{[w]} \circ (x + w') \\ &= (x - (f(w' + w) - f(w))) \circ (x - f(w)) \circ f \circ (x + w) \circ (x + w')\end{aligned}$$

$$= (x - f(w' + w)) \circ f \circ (x + w' + w) = f^{[w'+w]}.$$

Furthermore, for the derivative we have $(f^{[w]})' = f' \circ (x + w)$. Shifting respects decompositions in the sense that for each decomposition (g, h) of f we have a decomposition $(g^{[h(w)]}, h^{[w]})$ of $f^{[w]}$, and vice versa. We denote $(g^{[h(w)]}, h^{[w]})$ as $(g, h)^{[w]}$.

4.2 EXPLICIT COLLISIONS AT DEGREE r^2

> A good theorem has two proofs
> and one counterexample.
> — Volker Strassen

This section presents two classes of explicit collisions at degree r^2, where r is a power of the characteristic $p > 0$ of the field F. The collisions of Fact 4.2.1 consist of additive and subadditive polynomials. A polynomial A of degree r^κ is r-*additive* (or r-*linearized*) if it is of the form $A = \sum_{0 \leqslant i \leqslant \kappa} a_i x^{r^i}$ with all $a_i \in F$. We call a polynomial *additive* if it is p-additive. A polynomial is additive if and only if it acts additively on an algebraic closure $\overline{F}$ of F, that is $A(a+b) = A(a) + A(b)$ for all $a, b \in \overline{F}$; see Goss (1996, Corollary 1.1.6). The composition of additive polynomials is additive, see for instance Proposition 1.1.2 of the cited book. The decomposition structure of additive polynomials was first studied by Ore (1933). Dorey & Whaples (1974, Theorem 4) show that all components of an additive polynomial are additive. Giesbrecht (1988) gives lower bounds on the number of decompositions and algorithms to determine them.

For a divisor m of $r-1$, the (r, m)-*subadditive* (or (r, m)-*sublinearized*) polynomial associated with the r-additive polynomial A is given by $S = x(\sum_{0 \leqslant i \leqslant \kappa} a_i x^{(r^i-1)/m})^m$ of degree r^κ. Then A and S are related as $x^m \circ A = S \circ x^m$ and fall into the First Case of Ritt's Second Theorem. Dickson (1897) notes a special case of subadditive polynomials, and Cohen (1985) is concerned with the reducibility of some related polynomials. Cohen (1990a,b) investigates their connection to exceptional polynomials and coins the term "sub-linearized"; see also Cohen & Matthews (1994). Coulter, Havas & Henderson (2004) derive the number of indecomposable subadditive polynomials and present an algorithm to decompose subadditive polynomials.

Ore (1933, Theorem 3) describes exactly the right components of degree p of an additive polynomial. Henderson & Matthews (1999) relate such additive decompositions to subadditive polynomials, and in their Theorems 3.4 and 3.8 describe the collisions of Fact 4.2.1 below. The polynomials of Theorem 4.2.22 popped up in the course of trying to prove that these examples might be the only ones; see the proof of Theorem 4.4.9. In Section 4.4, we show that together with the Frobenius collisions of Example 4.1.4, these two examples and their shifts comprise all 2-collisions at degree p^2.

Fact 4.2.1. *Let* r *be a power of* p, $u, s \in F^\times$, $\varepsilon \in \{0, 1\}$, m *a positive divisor of* $r-1$, $\ell = (r-1)/m$, *and*

$$\begin{aligned} f &= S(u, s, \varepsilon, m) = x(x^{\ell(r+1)} - \varepsilon u s^r x^\ell + u s^{r+1})^m \in P_{r^2}(F), \\ T &= \{t \in F\colon t^{r+1} - \varepsilon u t + u = 0\}. \end{aligned} \tag{4.2.2}$$

For each $t \in T$ *and*

$$\begin{aligned} g &= x(x^\ell - u s^r t^{-1})^m, \\ h &= x(x^\ell - st)^m, \end{aligned} \tag{4.2.3}$$

both in $P_r(F)$, *we have* $f = g \circ h$. *Moreover,* f *has a* $\#T$*-collision.*

The polynomials f in (4.2.2) are "simply original" in the sense that they have a simple root at 0. This motivates the designation S.

Proof. For $t \in T$, we have

$$\begin{aligned} g \circ h &= x(x^\ell - st)^m (x^\ell (x^\ell - st)^{r-1} - u s^r t^{-1})^m \\ &= x(x^\ell (x^\ell - st)^r - (x^\ell - st) u s^r t^{-1})^m \\ &= x(x^{\ell r + \ell} - s^r t^r x^\ell - u s^r t^{-1} x^\ell + u s^{r+1})^m \\ &= x(x^{\ell(r+1)} - s^r (t^r + u t^{-1}) x^\ell + u s^{r+1})^m \\ &= x(x^{\ell(r+1)} - \varepsilon u s^r x^\ell + u s^{r+1})^m = f. \end{aligned}$$

This proves that (g, h) is a decomposition of f. While f does not depend on t, the $\#T$ different choices for t yield $\#T$ pairwise different values for the coefficients of $x^{r-\ell}$ in h, namely

$$h_{r-\ell} = -mst \neq 0. \qquad \square$$

The polynomial $S(u, s, \varepsilon, m)$ is r-additive for $m = 1$ and (r, m)-subadditive for all m. Bluher (2004) shows that for $\varepsilon = 1$ and $F \cap \mathbb{F}_r$ of size Q, the cardinality of T is either 0, 1, 2, or $Q+1$. This also holds for $\varepsilon = 0$. In either case, T is independent of m and ℓ. If T is empty, then $S(u, s, \varepsilon, m)$ has no decomposition of the form (4.2.3), but $r+1$ such decompositions exist over the splitting field of the squarefree polynomial $y^{r+1} - \varepsilon u y + u \in F[y]$.

For a polynomial $f \in P_n(F)$ and an integer i, we denote the coefficient of x^i in f by f_i, so that $f = x^n + \sum_{1 \leqslant i < n} f_i x^i$ with $f_i \in F$. The *second degree* of f is

$$\deg_2 f = \deg(f - x^n). \tag{4.2.4}$$

If $p \mid n$ and $p \nmid \deg_2 f$, then $\deg_2 f = \deg(f') + 1$.

Fact 4.2.5 (von zur Gathen, Giesbrecht & Ziegler (2010), Proposition 6.2)**.** *Let* r *be a power of* p, *and* u, s, ε, m *and* u^*, s^*, ε^*, m^* *satisfy the conditions of Fact 4.2.1. For* $f = S(u, s, \varepsilon, m)$ *and* $f^* = S(u^*, s^*, \varepsilon^*, m^*)$, *the following hold.*

(i) *For $\varepsilon = 1$, we have $f = f^*$ if and only if*

$$(u, s, \varepsilon, m) = (u^*, s^*, \varepsilon^*, m^*).$$

(ii) *For $\varepsilon = 0$, we have $f = f^*$ if and only if*

$$(us^{r+1}, \varepsilon, m) = (u^*(s^*)^{r+1}, \varepsilon^*, m^*).$$

(iii) *The stabilizer of f under original shifting is F if $m = 1$, and $\{0\}$ otherwise. For $F = \mathbb{F}_q$, the orbit of f under original shifting has size 1 if $m = 1$, and size q otherwise.*

(iv) *The only polynomial of the form* (4.2.2) *in the orbit of f under original shifting is f itself.*

Proof. The appearance of $O(x^i)$ for some integer i in an equation means the existence of some polynomial of degree at most i that makes the equation valid.

Let $\ell = (r-1)/m$. Then $\gcd(r, \ell) = \gcd(r, m) = 1$ and $\ell m \equiv -1 \bmod p$. We have

$$\begin{aligned} f &= x(x^{\ell(r+1)} - \varepsilon u s^r x^\ell + u s^{r+1})^m \\ &= x(x^{r^2-1} - m\varepsilon u s^r x^{r^2-\ell r-1} \\ &\quad + mu s^{r+1} x^{r^2-\ell r-\ell-1} + O(x^{r^2-2\ell r-1})) \\ &= x^{r^2} - m\varepsilon u s^r x^{r^2-\ell r} \\ &\quad + mu s^{r+1} x^{r^2-\ell r-\ell} + O(x^{r^2-2\ell r}), \qquad (4.2.6) \\ f_{r^2-\ell r} &= -m\varepsilon u s^r, \qquad (4.2.7) \\ f_{r^2-\ell r-\ell} &= mu s^{r+1} \neq 0, \qquad (4.2.8) \\ \deg_2 f &= \begin{cases} r^2 - \ell r & \text{if } \varepsilon = 1, \\ r^2 - \ell r - \ell & \text{if } \varepsilon = 0. \end{cases} \qquad (4.2.9) \end{aligned}$$

From the last equation, we find $\varepsilon = 1$ if $r \mid \deg_2 f$, and $\varepsilon = 0$ otherwise. For either value of ε, $\deg_2 f$ determines ℓ and $m = (r-1)/\ell$ uniquely. Similarly, $\deg_2 f^*$ determines ε^*, ℓ^*, and m^* uniquely. Therefore, if $\deg_2 f = \deg_2 f^*$, then

$$(\varepsilon, \ell, m) = (\varepsilon^*, \ell^*, m^*). \qquad (4.2.10)$$

Furthermore, m and the coefficient $f_{r^2-\ell r-\ell}$ determine $us^{r+1} = f_{r^2-\ell r-\ell}/m$ uniquely by (4.2.8). Similarly, m^* and $f^*_{r^2-\ell^* r-\ell^*}$ determine $u^*(s^*)^{r+1}$ uniquely. Thus, if $m = m^*$ and $f_{r^2-\ell r-\ell} = f^*_{r^2-\ell^* r-\ell^*}$, then

$$us^{r+1} = u^*(s^*)^{r+1}. \qquad (4.2.11)$$

(i) If $(u, s, \varepsilon, m) = (u^*, s^*, \varepsilon^*, m^*)$, then $f = f^*$. On the other hand, we have $f_{r^2-\ell r} = -mus^r \neq 0$ in (4.2.7) and with (4.2.8) this determines uniquely

$$\begin{aligned} s &= -f_{r^2-\ell r-\ell}/f_{r^2-\ell r}, \\ u &= -f_{r^2-\ell r}/ms^r = \ell f_{r^2-\ell r}/s^r. \end{aligned} \tag{4.2.12}$$

This implies the claim (i).

(ii) The condition $(us^{r+1}, \varepsilon, m) = (u^*(s^*)^{r+1}, \varepsilon^*, m^*)$ is sufficient for $f = f^*$ by direct computation from (4.2.2). It is also necessary by (4.2.10) and (4.2.11).

(iii) For $m = 1$, f is r-additive as noted after the proof of Fact 4.2.1 and $f^{[w]} = f$ for all $w \in F$. For $m > 1$ and $w \in F$, we find

$$\begin{aligned} f^{[w]} = x^{r^2} &- m\varepsilon us^r x^{r^2-\ell r} + mus^{r+1}x^{r^2-\ell r-\ell} \\ &+ wus^{r+1}x^{r^2-\ell r-\ell-1} + O(x^{r^2-\ell r-\ell-2}), \end{aligned} \tag{4.2.13}$$

$$f^{[w]}_{r^2-\ell r} = f_{r^2-\ell r} = -m\varepsilon us^r, \tag{4.2.14}$$

$$f^{[w]}_{r^2-\ell r-\ell} = f_{r^2-\ell r-\ell} = mus^{r+1} \neq 0, \tag{4.2.15}$$

$$f^{[w]}_{r^2-\ell r-\ell-1} = wus^{r+1}. \tag{4.2.16}$$

We have $f = f^{[0]}$ by definition and $f \neq f^{[w]}$ for $w \neq 0$ by (4.2.16) and $us^{r+1} \neq 0$.

(iv) For $m = 1$, the claim follows from (iii). For $m > 1$ and $w \in F$, assume $f_0 = S(u_0, s_0, \varepsilon_0, m_0) = f^{[w]}$ for parameters $u_0, s_0, \varepsilon_0, m_0$ satisfying the conditions of Fact 4.2.1. Then $\deg_2 f_0 = \deg_2 f^{[w]}$ by assumption and

$$\deg_2 f^{[w]} = \deg_2 f = \begin{cases} r^2 - \ell r & \text{if } \varepsilon = 1, \\ r^2 - \ell r - \ell & \text{if } \varepsilon = 0, \end{cases} \tag{4.2.17}$$

from (4.2.13) and (4.2.9). Thus, we have $\ell = \ell_0$ by (4.2.10). The coefficient of $x^{r^2-\ell r-\ell-1}$ is 0 in f_0 and wus^{r+1} in $f^{[w]}$ by (4.2.6) and (4.2.16), respectively. With $us^{r+1} \neq 0$, we have $w = 0$ and $f_0 = f^{[0]} = f$. □

Algorithm 4.2.18 identifies the examples of Fact 4.2.1 and their shifts. The algorithm involves divisions which we execute conditionally "if defined". Namely, for integers the quotient is returned, if it is an integer, and for field elements, if the denominator is nonzero. Otherwise, "failure" is returned. Besides the field operations $+$, $-$, $\cdot$, we assume a routine for computing the number of roots in F of a polynomial. Furthermore, we denote by $M(n)$ a number of field operations which is sufficient to compute the product of two polynomials of degree at most n.

Theorem 4.2.19. *Algorithm 4.2.18 works correctly as specified. If* $F = \mathbb{F}_q$, *it takes* $O(M(n)\log(nq))$ *field operations on input a polynomial of degree* $n = r^2$.

Algorithm 4.2.18: Identify simply original polynomials

Input: a polynomial $f = \sum_i f_i x^i \in P_{r^2}(F)$ with all $f_i \in F$ and r a power of $\operatorname{char} F$

Output: integer k, parameters u, s, ε, m as in Fact 4.2.1, and $w \in F$ such that $f = S(u, s, \varepsilon, m)^{[w]}$ has a k-collision with $k = \#T$ as in (4.2.2), if such values exist, and "failure" otherwise

if $\deg_2 f = -\infty$ **then return** *"failure"*
if $r \mid \deg_2 f$ **then**
  $\varepsilon \leftarrow 1$
  $\ell \leftarrow (r^2 - \deg_2 f)/r$ and $m \leftarrow (r-1)/\ell$ if defined
  $s \leftarrow -f_{r^2-\ell r-\ell}/f_{r^2-\ell r}$ if defined
else
  $\varepsilon \leftarrow 0$
  $\ell \leftarrow (r^2 - \deg_2 f)/(r+1)$ and $m \leftarrow (r-1)/\ell$ if defined
  $s \leftarrow 1$
end
$u \leftarrow -\ell f_{r^2-\ell r-\ell}/s^{r+1}$ if defined
if $us = 0$ **then return** *"failure"*
$w \leftarrow m f_{r^2-\ell r-\ell-1}/f_{r^2-\ell r-\ell}$ if defined
if $f = S(u, s, \varepsilon, m)^{[w]}$ **then**
  $k \leftarrow \#\{y \in F\colon y^{r+1} - \varepsilon u y + u = 0\}$
  return $k, u, s, \varepsilon, m, w$
end
return *"failure"*

Proof. For the first claim, we show that for $u_0, s_0, \varepsilon_0, m_0$ as in Fact 4.2.1 and $w_0 \in F$ the algorithm does not return "failure" on input $f = S(u_0, s_0, \varepsilon_0, m_0)^{[w_0]}$.

We have $\deg_2 f > 0$ by (4.2.17). Thus, step 1 does not return "failure". By the same equation, we have $r \mid \deg_2 f$ if and only if $\varepsilon_0 = 1$. Therefore, $\varepsilon = \varepsilon_0$ after step 3 or 7, respectively, and since (4.2.17) determines $\ell_0 = (r-1)/m_0$ uniquely, we find $\ell = \ell_0$ and $m = (r-1)/\ell_0 = m_0$ after step 4 or 8, respectively. If $\varepsilon = 1$, then step 5 computes $s = s_0$ from (4.2.12), (4.2.14), and (4.2.15). Furthermore, step 11 computes $u = u_0$ from (4.2.8) and (4.2.15). If $\varepsilon = 0$, then

$$S(u_0, s_0, 0, m)^{[w_0]} = (x(x^{\ell(r+1)} + u_0 s_0^{r+1})^m)^{[w_0]} = S(u_0 s_0^{r+1}, 1, 0, m)^{[w_0]}. \tag{4.2.20}$$

Therefore, we can choose $s = 1$ in step 9 and set $u = -\ell f_{r^2-\ell r-\ell} = u_0 s_0^{r+1}$ by (4.2.8) and (4.2.15) in step 11. For either value of ε, we have $us \neq 0$ from $u_0 s_0 \neq 0$ and step 12 does not return "failure".

For $m = 1$, we have

$$S(u, s, \varepsilon, 1)^{[w_0]} = S(u, s, \varepsilon, 1)^{[0]}$$

by Fact 4.2.5 (iii) and $w = f_0/f_1 = 0$ in step 13 is a valid choice. For $m > 1$, we find w_0 from (4.2.15) and (4.2.16) as

$$w = m f_{r^2-\ell r-\ell-1}/f_{r^2-\ell r-\ell} = w_0.$$

A polynomial f of the assumed form passes the final test in step 14, while an f not of this form will fail here at the latest. The size k of the set $T = \{t \in F\colon t^{r+1} - \varepsilon u t + u = 0\}$ is computed in step 15 and f is a k-collision according to Fact 4.2.1.

In the following cost estimate for $F = \mathbb{F}_q$, we ignore the (cheap) operations on integers. The calculation of the right-hand side in step 14 takes $O(M(n)\log n)$ field operations, and the test another n operations. In step 15, we compute k as $\deg_y(\gcd(y^q - y, y^{r+1} - \varepsilon u y + u))$ with $O(M(r)(\log q + \log r))$ field operations. The cost of all other steps is dominated by these bounds. □

Let $C^{(S)}_{n,k}(F)$ denote the set of polynomials in $P_n(F)$ that are shifts of some $S(u, s, \varepsilon, m)$ with T as in (4.2.2) of cardinality k. Over a finite field, $\#C^{(S)}_{r^2,k}(\mathbb{F}_q)$ can be computed exactly, as in von zur Gathen, Giesbrecht & Ziegler (2010, Corollary 6.3).

Proposition 4.2.21. *Let r be a power of p, q a power of r, and τ the number of positive divisors of $r-1$. For $k \geqslant 2$, we have*

$$\#C^{(S)}_{r^2,k}(\mathbb{F}_q) = \begin{cases} \dfrac{(\tau q - q + 1)(q-1)^2(r-2)}{2(r-1)} & \text{if } k = 2, \\ \dfrac{(\tau q - q + 1)(q-1)(q-r)}{r(r^2-1)} & \text{if } k = r+1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We count the polynomials in $C^{(S)}_{r^2,k}(\mathbb{F}_q)$ by counting the admissible parameters u, s, ε, m, w modulo the ambiguities described in Fact 4.2.5.

For $\varepsilon = 1$, we count the possible $u \in \mathbb{F}_q^\times$ such that $y^{r+1} - uy + u \in \mathbb{F}_q[y]$ has exactly k roots in $\mathbb{F}_q$. Let $a, b \in \mathbb{F}_q^\times$ and $u = a^{r+1}b^{-r}$. The invertible transformation $x \mapsto y = -ab^{-1}x$ gives a bijection

$$\{x \in \mathbb{F}_q^\times : x^{r+1} + ax + b = 0\} \leftrightarrow \{y \in \mathbb{F}_q^\times : y^{r+1} - uy + u = 0\}.$$

Theorem 5.1 and Proposition 5.4 of von zur Gathen, Giesbrecht & Ziegler (2010) determine the number $c^{(2)}_{q,r,k}$ of pairs $(a, b) \in (\mathbb{F}_q^\times)^2$ such that $x^{r+1} + ax + b$ has exactly k roots, as described below. Every value of u corresponds to exactly $q-1$ pairs (a, b), namely an arbitrary $a \in \mathbb{F}_q^\times$ and b uniquely determined by $b^r = u^{-1}a^{r+1}$. Hence, there are exactly $c^{(2)}_{q,r,k}/(q-1)$ values for u where $\#T = k$. For $m = 1$, the orbit under original shifting has size 1 by Fact 4.2.5 (iii) and taking into account the $q-1$ possible choices for s we find that there are $c^{(2)}_{q,r,k}$ polynomials of the form $S(u, s, 1, 1)^{[w]}$. For $m > 1$, the orbit under original shifting contains exactly one polynomial of the form (4.2.2) by Fact 4.2.5 (iv) and has size q by (iii). Taking into account the $q-1$ choices for s and the $\tau - 1$ possible values for m, we find that there are $c^{(2)}_{q,r,k} \cdot (\tau - 1) \cdot q$ polynomials of the form $S(u, s, 1, m)^{[w]}$.

For $\varepsilon = 0$, we have $S(u, s, 0, m)^{[w]} = S(us^{r+1}, 1, 0, m)^{[w]}$ as in (4.2.20) and $T = \{t \in \mathbb{F}_q : t^{r+1} + us^{r+1} = 0\}$ as in (4.2.2). This set has exactly $\gamma = \gcd(r+1, q-1)$ elements, if $-u$ is an $(r+1)$st power, and is empty otherwise. Then $\#T = k \geqslant 2$ if and only if $k = \gamma$ and $-u$ is an $(r+1)$st power. There are exactly $(q-1)/\gamma$ distinct $(r+1)$st powers in $\mathbb{F}_q^\times$ and therefore exactly $(q-1)/\gamma$ distinct values for us^{r+1} such that $\#T = \gamma$. With δ being Kronecker's delta function, we find, as above, that there are $\delta_{\gamma,k} \cdot (q-1)/\gamma$ polynomials of the form $S(u, s, 0, 1)^{[w]}$ in $C^{(S)}_{r^2,k}(\mathbb{F}_q)$ and $\delta_{\gamma,k} \cdot (\tau - 1)q(q-1)/\gamma$ of the form $S(u, s, 0, m)^{[w]}$ with $m > 1$.

This yields

$$\#C^{(S)}_{r^2,k}(\mathbb{F}_q) = (\tau q - q + 1) \cdot \left(c^{(2)}_{q,r,k} + \delta_{\gamma,k} \frac{q-1}{\gamma} \right).$$

The work cited above provides the following explicit expressions for $k \geqslant 2$, with $q = r^d$:

$$c^{(2)}_{q,r,2} = \begin{cases} \dfrac{(q-1)(qr - 2q - 2r + 3)}{2(r-1)} & \text{if } q \text{ and } d \text{ are odd,} \\ \dfrac{(q-1)^2(r-2)}{2(r-1)} & \text{otherwise,} \end{cases}$$

$$c^{(2)}_{q,r,r+1} = \begin{cases} \dfrac{(q-1)(q-r^2)}{r(r^2-1)} & \text{if } d \text{ is even,} \\ \dfrac{(q-1)(q-r)}{r(r^2-1)} & \text{if } d \text{ is odd,} \end{cases}$$

and $c^{(2)}_{q,r,k} = 0$ for $k \notin \{2, r+1\}$. Furthermore, we have from Lemma 3.29 in von zur Gathen (2014a, Preprint)

$$\gamma = \gcd(r+1, r^d - 1) = \begin{cases} 1 & \text{if } d \text{ is odd and } r \text{ is even,} \\ 2 & \text{if } d \text{ is odd and } r \text{ is odd,} \\ r+1 & \text{if } d \text{ is even.} \end{cases}$$

The claimed formulas follow from

$$c^{(2)}_{q,r,k} + \delta_{\gamma,k}\frac{q-1}{\gamma} = \begin{cases} \dfrac{(q-1)^2(r-2)}{2(r-1)} & \text{if } k = 2, \\ \dfrac{(q-1)(q-r)}{r(r^2-1)} & \text{if } k = r+1, \\ 0 & \text{otherwise.} \end{cases} \qquad \square$$

For a prime $p \geqslant 7$, we have $\tau \geqslant 4$. Large values of τ occur when $m \approx \exp(k \log k)$ is the product of the first k primes and $p \leqslant m^C$ the smallest prime congruent 1 mod m for Linnik's constant C. Then $k \approx \log m / \operatorname{loglog} m \gtrsim C^{-1} \log p / \operatorname{loglog} p$ and $\tau \geqslant 2^k \gtrsim 2^{C^{-1} \log p / \operatorname{loglog} p}$. By Heath-Brown (1992) and Xylouris (2011) we can take C just under 5. Except for the constant factor, τ is asymptotically not more than this value (Hardy & Wright, 1985, Theorem 317). Luca & Shparlinski (2008) give general results on the possible values of τ. It follows that $\#C^{(S)}_{r^2,2}(\mathbb{F}_q) \approx \tau q^3/2$ is in $q^3 O(p^{1/\operatorname{loglog} p})$.

The odd/even distinctions for q, r, and d cancel out in the formula of Proposition 4.2.21. This might indicate that those distinctions are alien to the problem.

The second and new construction of collisions goes as follows.

Theorem 4.2.22. *Let r be a power of p, $b \in F^\times$, $a \in F \setminus \{0, b^r\}$, $a^* = b^r - a$, m an integer with $1 < m < r-1$ and $p \nmid m$, $m^* = r - m$, and*

$$\begin{aligned} f = M(a, b, m) &= x^{mm^*}(x-b)^{mm^*}\left(x^m + a^* b^{-r}((x-b)^m - x^m)\right)^m \\ &\quad \cdot \left(x^{m^*} + ab^{-r}((x-b)^{m^*} - x^{m^*})\right)^{m^*}, \\ g &= x^m(x-a)^{m^*}, \\ h &= x^r + a^* b^{-r}(x^{m^*}(x-b)^m - x^r), \\ g^* &= x^{m^*}(x-a^*)^m, \\ h^* &= x^r + ab^{-r}(x^m(x-b)^{m^*} - x^r). \end{aligned} \tag{4.2.23}$$

Then $f = g \circ h = g^* \circ h^* \in P_{r^2}(F)$ has a 2-collision.

The polynomials f in (4.2.23) are "multiply original" in the sense that they have a multiple root at 0. This motivates the designation M. The notation is set up so that * acts as an involution on our data, leaving b, f, r, and x invariant.

Avanzi & Zannier (2003) study collisions $g \circ h = g \circ h^*$ with a polynomial g and nonconstant rational functions h, h^* over $\mathbb{C}$. Mike Zieve (2011) points out that the rational functions of case (4) in their Proposition 5.6 can be transformed into (4.2.23). Zieve also mentions that this example already occurs in unpublished work of his, joint with Bob Beals.

Proof. Let

$$\begin{aligned} H &= h/x^{m^*} = x^m + a^* b^{-r}((x-b)^m - x^m), \\ H^* &= h^*/x^m = x^{m^*} + a b^{-r}((x-b)^{m^*} - x^{m^*}). \end{aligned} \tag{4.2.24}$$

Then $h - a = (x-b)^m H^*$ and $h^* - a^* = (x-b)^{m^*} H$. It follows that

$$g \circ h = g^* \circ h^* = x^{mm^*}(x-b)^{mm^*} H^m (H^*)^{m^*} = f. \tag{4.2.25}$$

If $g = g^*$, then the coefficients of x^{r-1} in g and g^* yield $mb^r = 0$, hence $p \mid m$, a contradiction. Thus f is a 2-collision. □

For $r \leqslant 4$, there is no value of m satisfying the assumptions. The construction works for arbitrary $a \in F$ and $1 \leqslant m \leqslant r-1$. But when $a \in \{0, b^r\}$, we get a Frobenius collision; see Example 4.1.4. When $p \mid m$, we write $m = p^e m_0$ with $p \nmid m_0$ and have $f = x^{p^e} \circ M(a, b^{p^e}, m_0) \circ x^{p^e}$ with r/p^e instead of r in (4.2.23). When m is 1 or $r-1$, an original shift of (4.2.23) yields a polynomial of the form $S(u, s, \varepsilon, m)$. Indeed, for $m = 1$, let $w = a^* b^{-r+1}$, $c = (ab^{1-r})^r - a^*$, and

$$(u, s, \varepsilon, m, t, t^*) = \begin{cases} (-aa^* b^{1-r}, 1, 0, r-1, -a^* b^{1-r}, ab^{1-r}) & \text{if } c = 0, \\ (c/s^r, -aa^* b^{1-r}/c, 1, r-1, -c/a, c/a^*) & \text{otherwise.} \end{cases}$$

Then $M(a, b, 1)^{[w]} = S(u, s, \varepsilon, m)$, $(g, h)^{[w]}$ is of the form (4.2.3), and so is $(g^*, h^*)^{[w]}$ with t replaced by t^*. Furthermore, for $m = r-1$, we have $M(a, b, r-1) = M(a^*, b, 1)$ and the claimed parameters can be found as described by interchanging a and a^*.

Next, we describe the (non)uniqueness of this construction. We take all polynomial gcds to be monic, except that $\gcd(0, 0) = 0$.

Proposition 4.2.26. *Let r be a power of p, $b \in F^\times$, $a \in F \setminus \{0, b^r\}$, m an integer with $1 < m < r-1$ and $p \nmid m$, and $f = M(a, b, m)$ as in (4.2.23). Then the following hold.*

(i) In the notation of Theorem 4.2.22 and with H and H^* as in (4.2.24), we have $\gcd(m, m^*) = 1$ and the four polynomials x, $x - b$, H, and H^* are squarefree and pairwise coprime.

(ii) The stabilizer of f under original shifting is $\{0\}$. For $F = \mathbb{F}_q$, the orbit of f under original shifting has size q.

(iii) *For* a_0, b_0, m_0 *satisfying the conditions of Theorem 4.2.22, we have* $M(a,b,m) = M(a_0,b_0,m_0)$ *if and only if* $(a_0,b_0,m_0) \in \{(a,b,m), (a^*,b,m^*)\}$. *If we impose the additional condition* $m < r/2$, *then* (a,b,m) *is uniquely determined by* $M(a,b,m)$.

(iv) *There are exactly two polynomials of the form* (4.2.23) *in the orbit of* f *under original shifting, namely* f *and* $f^{[b]} = M(-a^*,-b,m)$.

Proof. (i) If $d > 1$ was a common divisor of m and m^*, then $d \mid m + m^* = r$ and thus d would be a power of p—in particular $p \mid m$, a contradiction. Thus $\gcd(m,m^*) = 1$. From $mH - xH' = m^*a^*b^{1-r}(x-b)^{m-1}$ and $H(0)\cdot H(b) \neq 0$, we find that H is squarefree and coprime to $x(x-b)$, and similarly for H^*. Since $H \mid h$, $H^* \mid (h-a)$, and $\gcd(h, h-a) = 1$, we have $\gcd(H,H^*) = 1$.

(ii) For the coefficient of x^{r^2-r-2} in the composition $f = g \circ h$, we find

$$f_{r^2-r-2} = g_{r-1}(h_{r-1}^2 - h_{r-2}),$$

since $r > 2$. For the shifted composition $f^{[w]} = g^{[h(w)]} \circ h^{[w]}$, we have the coefficients

$$\begin{aligned} g_{r-1}^{[h(w)]} &= g_{r-1} = -m^*a \neq 0,\\ h_{r-1}^{[w]} &= h_{r-1} = -ma^*(-b)^{1-r} \neq 0,\\ h_{r-2}^{[w]} &= h_{r-2} - wh_{r-1},\\ f_{r^2-r-2}^{[w]} &= g_{r-1}(h_{r-1}^2 - h_{r-2} + wh_{r-1}). \end{aligned}$$

Thus, $f_{r^2-r-2} = f_{r^2-r-2}^{[w]}$ if and only if $w = 0$.

(iii) Sufficiency is a direct computation. Conversely, assume that $f = M(a,b,m) = M(a_0,b_0,m_0) = f_0$. From (i) and the multiplicity mm^* of 0 and b in f, we find $mm^* = m_0m_0^*$ and $b_0 = b$; see (4.2.25). If necessary, we replace (a,b,m) by (a^*,b,m^*), and obtain $m_0 = m$. Dividing f and f_0 by $x^{mm^*}(x-b)^{mm^*}$ yields $H^m(H^*)^{m^*} = H_0^m(H_0^*)^{m^*}$ by (4.2.25). Hence by (i), we find $H_0 = H$ and thus $a_0 = a$.

(iv) We find $f^{[b]} = M(-a^*,-b,m)$ by a direct computation. Conversely, we take a_0, b_0, m_0 as in Theorem 4.2.22 and assume that $f^{[w]} = M(a_0,b_0,m_0) = f_0$. By (iii), we may assume that $m, m_0 < r/2$. We have

$$\begin{aligned} g' &= m^*ax^{m-1}(x-a)^{m^*-1},\\ h' &= ma^*b^{1-r}x^{m^*-1}(x-b)^{m-1},\\ f' &= (g'\circ h)\cdot h'\\ &= mm^*aa^*b^{1-r}(x(x-b))^{mm^*-1}H^{m-1}(H^*)^{m^*-1}. \end{aligned} \tag{4.2.27}$$

Now (i) and $p \nmid mm^*$ show that f' has roots of multiplicity mm^*-1 exactly at 0 and b and otherwise only roots of multiplicity at most $m^*-1 < mm^*-1$. Furthermore, $(f^{[w]})' = f'(x+w)$ has roots of

multiplicity $mm^* - 1$ exactly at $-w$ and $b - w$. Similarly, f_0 has roots of multiplicity $m_0 m_0^* - 1$ at 0 and b_0, and all other roots have smaller multiplicity. It follows that $mm^* = m_0 m_0^*$ and $m = m_0$. Furthermore, one of $-w$ and $b - w$ equals 0, so that $w \in \{0, b\}$. Hence

$$(a_0, b_0, m_0, w) \in \{(a, b, m, 0), (a^*, b, m^*, 0), \\ (-a^*, -b, m, b), (-a, -b, m^*, b)\}. \quad \square$$

We now provide the exact number of these collisions over $\mathbb{F}_q$, matching Proposition 4.2.21. When $r \leqslant 4$, there are no polynomials of the form (4.2.23).

Corollary 4.2.28. *For $r \geqslant 3$ and $F = \mathbb{F}_q$, the number of polynomials that are of the form* (4.2.23) *or shifts thereof is*

$$\frac{q(q-1)(q-2)(r - \frac{r}{p} - 2)}{4}.$$

Proof. There are $q - 1$, $q - 2$, and $r - r/p - 2$ choices for the parameters b, a, and m, respectively. By Proposition 4.2.26 (iii), exactly two distinct triples of parameters generate the same polynomial (4.2.23). By (ii), the shift orbits are of size q and by (iv), they contain two such polynomials each. $\square$

Over a field F of characteristic $p > 0$, Algorithm 4.2.29 finds the parameters for polynomials that are original shifts of (4.2.23), just as Algorithm 4.2.18 does for original shifts of (4.2.2). It involves conditional divisions and routines for extracting pth and square roots. Given a field element, the latter produce a root, if one exists, and "failure" otherwise. If F is finite, then every element has a pth root. The algorithm for a square root yields a subroutine to determine the set of roots of a quadratic polynomial.

Theorem 4.2.30. *Algorithm 4.2.29 works correctly as specified. If $F = \mathbb{F}_q$, it takes $O(M(n) \log n + n \log q)$ field operations on input a polynomial of degree $n = r^2$.*

Proof. For the correctness, it is sufficient—due to the check in step 23—to show that for a_0, b_0, m_0 as in Theorem 4.2.22 and $w_0 \in F$, the algorithm does not return "failure" on input $f = M(a_0, b_0, m_0)^{[w_0]}$. As remarked after Theorem 4.2.22, we have $r \geqslant 5$ and by Proposition 4.2.26 (iii), we may assume $m_0 < r/2$. Furthermore, (4.2.27) determines $\mathrm{lc}(f') \neq 0$ explicitly and step 1 is defined. The square root in step 2 is defined, since for $p = 2$, m_0 and $r - m_0$ are odd and all exponents in the monic version of (4.2.27) are even.

By (4.2.27) and Proposition 4.2.26 (i), we have after steps 1 and 2

$$f_0 = \begin{cases} \varphi^{m_0(r-m_0)-1} H_0^{m_0-1} H_0^{*\,r-m_0-1} & \text{if } p > 2, \\ \varphi^{(m_0(r-m_0)-1)/2} H_0^{(m_0-1)/2} H_0^{*\,(r-m_0-1)/2} & \text{if } p = 2, \end{cases} \tag{4.2.31}$$

Algorithm 4.2.29: Identify multiply original polynomials

Input: a polynomial $f \in P_{r^2}(F)$ with r a power of $p = \operatorname{char} F$
Output: parameters a, b, m, as in Theorem 4.2.22, and $w \in F$ such that $f = M(a, b, m)^{[w]}$, if such values exist, and "failure" otherwise

$f_0 \leftarrow f'/\operatorname{lc}(f')$ if defined
if $p = 2$ **then** $f_0 \leftarrow f_0^{1/2}$ if defined
$f_1 \leftarrow f_0/\gcd(f_0, f_0')$ if defined
if $\deg f_1 < 4$ **or** $\deg f_1 > r + 2$ **then return** *"failure"*
determine the maximal k such that $f_1^k \mid f_0$ via the generalized Taylor expansion of f_0 in base f_1
if $p = 2$ **then** $k \leftarrow 2k$
$m \leftarrow \min\{k + 1, r - k - 1\}$
if $m < 2$ **then return** *"failure"*
if $p = 2$ *or* $p \nmid m^2 + 1$ **then**
  $f_2 \leftarrow \gcd(f_1^{r-m}, f_0)/\gcd(f_1^{r-m-1}, f_0)$
else
  $f_3 \leftarrow f_0/\gcd(f_1^{r-m-1}, f_0)$ if defined
  determine the maximal ℓ such that p^ℓ divides every exponent of x with nonzero coefficient in f_3
  $f_3 \leftarrow f_3^{1/p^\ell}$ if defined
  $f_2 \leftarrow f_3/\gcd(f_3, f_3')$
end
if $\deg f_2 \neq 2$ **then return** *"failure"*
compute the set X of roots of f_2 in F
if $\#X < 2$ **then return** *"failure"*
write X as $\{x_1, x_2\}$ and set $b \leftarrow x_2 - x_1$ and $w \leftarrow -x_1$
compute the set A of roots of $y^2 - b^r y - m^{-2} b^{r-1} \operatorname{lc}(f') \in F[y]$ in F
for $a \in A$ **do**
  if $f = M(a, b, m)^{[w]}$ **then**
    return a, b, m, w
  end
end
return *"failure"*

with $\varphi = (x + w_0)(x - b_0 + w_0)$, $H_0 = H \circ (x + w_0)$, $H_0^* = H^* \circ (x + w_0)$, and H and H^* as in (4.2.24) with $a_0, a_0^*, b_0, m_0, m_0^*$ instead of a, a^*, b, m, m^*, respectively. By Proposition 4.2.26 (i), these three polynomials are squarefree and pairwise coprime. Let δ, ε, ε^* be 0 if p divides the exponent of φ, H_0, H_0^*, respectively, in (4.2.31), and be 1 otherwise. Then

$$\gcd(f_0, f_0') = \begin{cases} \varphi^{m_0(r-m_0)-1-\delta} H_0^{m_0-1-\varepsilon} H_0^{*\,r-m_0-1-\varepsilon^*} & \text{if } p > 2, \\ \varphi^{(m_0(r-m_0)-1)/2-\delta} H_0^{(m_0-1)/2-\varepsilon} & \\ \quad \cdot H_0^{*\,(r-m_0-1)/2-\varepsilon^*} & \text{if } p = 2. \end{cases}$$

This gcd is nonzero, and step 3 computes

$$f_1 = f_0 / \gcd(f_0, f_0') = \varphi^{\delta} H_0^{\varepsilon} H_0^{*\,\varepsilon^*}.$$

We have

$$\delta = \begin{cases} 1 & \text{if } p = 2 \text{ or } p \nmid m_0^2 + 1, \\ 0 & \text{otherwise.} \end{cases} \tag{4.2.32}$$

For odd p, this follows from $m_0(r - m_0) - 1 \equiv -m_0^2 - 1 \bmod p$, and for $p = 2$ from $4 \nmid m_0^2 + 1$. The sum of the exponents of H_0 and H_0^* in (4.2.31) is $r - 2$ for odd p and $r/2 - 1$ for $p = 2$. In either case, it is coprime to p and at least one of ε and ε^* equals 1. If $p > 2$ and $\varepsilon = 0$, then $m_0 \equiv 1 \bmod p$, and thus $m_0^2 \equiv 1 \bmod p$. Hence $p \nmid m_0^2 + 1$ and $\delta = 1$. Similarly, $\varepsilon^* = 0$ implies $\delta = 1$, and we find that at least two of δ, ε, and ε^* take the value 1. This also holds for $p = 2$.

Since $\deg \varphi = 2$, $\deg H_0, \deg H_0^* \geqslant 2$, and $\deg H_0 + \deg H_0^* = r$, this implies $4 \leqslant \deg f_1 \leqslant r + 2$ and step 4 does not return "failure". The exponents in (4.2.31) satisfy $m_0 - 1 < r - m_0 - 1 < m_0(r - m_0) - 1$. If $p > 2$, then k as determined in step 5 equals $m_0 - 1$ if $\varepsilon = 1$, and $r - m_0 - 1$ otherwise. In characteristic 2, step 6 modifies $k \in \{(m_0 - 1)/2, (r - m_0 - 1)/2\}$, so that in any characteristic, step 7 recovers $m = m_0 \geqslant 2$ and step 8 does not return "failure".

The condition in step 9 reflects the case distinction in (4.2.32).

- If the condition holds, we have $\delta = 1$ and

$$\gcd(f_1^{r-m}, f_0) = \varphi^{r-m} H_0^{\varepsilon(m-1)} H_0^{*\,\varepsilon^*(r-m-1)},$$
$$\gcd(f_1^{r-m-1}, f_0) = \varphi^{r-m-1} H_0^{\varepsilon(m-1)} H_0^{*\,\varepsilon^*(r-m-1)},$$

  and therefore $f_2 = \varphi$ in step 10.

- Otherwise, we have $\delta = 0$, $p > 2$, $\varepsilon = \varepsilon^* = 1$,

$$f_0 = \varphi^{m(r-m)-1} H_0^{m-1} H_0^{*\,r-m-1},$$
$$\gcd(f_1^{r-m-1}, f_0) = H_0^{m-1} H_0^{*\,r-m-1},$$

  and $f_3 = \varphi^{m(r-m)-1}$ in step 12. After step 14, we have $f_3 = \varphi^e$ for some e with $p \nmid e$ and $f_2 = \varphi^e / \varphi^{e-1} = \varphi$ in step 15.

In any case, we have $f_2 = (x + w_0)(x - b_0 + w_0)$ with distinct roots $-w_0$ and $b_0 - w_0$ in F, and steps 17, 18, and 19 do not return "failure". We determine a, b, and w in steps 20–23. In step 20, we have $(b, w) \in \{(b_0, w_0), (-b_0, w_0 - b_0)\}$, depending on the choice of the order of x_1 and x_2. Since $f = M(a_0, b_0, m)^{[w_0]} = M(b_0^r - a_0, -b_0, m)^{[w_0 - b_0]}$ according to Proposition 4.2.26 (iv), we have $f = M(\bar{a}, b, m)^{[w]}$ for some $\bar{a} \in \{a_0, b_0^r - a_0\}$. The leading coefficient of f' is $-m^2 \bar{a} b^{1-r}(b^r - \bar{a})$ by (4.2.27) yielding a quadratic polynomial in $F[y]$ with roots $\bar{a}$ and $b^r - \bar{a}$ for step 21. There, we find $A = \{\bar{a}, b^r - \bar{a}\}$ and step 23 identifies $\bar{a}$.

For the cost over $F = \mathbb{F}_q$, the conditions in steps 4 and 8 ensure that all powers of f_1 in the gcd computations of steps 10 and 12 have degree at most $(r + 2)(r - 2) < n$ and we have $O(M(n) \log n)$ field operations for the quotients, gcds, and products in steps 1, 3, 10, 12, 15, and 23. The f_1-adic expansion of f_0 is a sequence $a_0, \dots, a_{\nu-1} \in \mathbb{F}_q[x]$ such that $f_0 = \sum_{0 \leqslant i < \nu} a_i f_1^i$ and $\deg a_i < \deg f_1$ for all $i < \nu$. We may bound ν by the smallest power of 2 greater than $\deg f_0 / \deg f_1$. Then $\nu < 2 \deg f_0 / \deg f_1$ and for k in step 5 we have $k + 1 = \min\{0 \leqslant i < \nu \colon a_i \neq 0\}$. We can compute the expansion with $O(M(\nu \deg f_1) \log \nu)$ field operations; see von zur Gathen & Gerhard (2013, Theorem 9.15). Thus the cost of step 5 is $O(M(n) \log n)$ field operations. The calculation of the right-hand side in step 23 takes $O(M(n) \log n)$ field operations, by first substituting $x + w$ for x in $M(a, b, m)$ as in (4.2.23), then computing its coefficients and leaving away the constant term. We ignore the (cheap) operations on integers in the various tests, in step 13, and the computation of derivatives in steps 1, 3, and 15. The polynomial square root in step 2 and the p^ℓth root in step 14 take $O(n \log q)$ field operations each using $u^{q^c/p^\ell} = u^{1/p^\ell}$ for $u \in \mathbb{F}_q$ and the smallest $c \geqslant 1$ with $q^c \geqslant p^\ell$. Taking the square roots in steps 18 and 21 can be done deterministically by first reducing the computations to the prime field $\mathbb{F}_p$, see von zur Gathen & Gerhard (2013, Exercise 14.40), and then finding square roots in $\mathbb{F}_p$ by exhaustive search. These take $O(\log q)$ and $O(\sqrt{n})$ field operations, respectively, since $n = r^2$ is a power of p. □

4.3 ROOT MULTIPLICITIES IN COLLISIONS

> The aim of research
> is the discovery of the equations
> which subsist between the elements of phenomena.
> — Ernst Mach

In this section we describe the structure of root multiplicities in collisions over an algebraic closure of F under certain conditions. In Section 4.4 these results will be used for the classification of 2-collisions at degree p^2. For the classification, its proof, and the lem-

mas in this section, we follow ideas of Dorey & Whaples (1974) and Zannier (1993); an earlier version can be found in Blankertz (2011).

After some general facts about root multiplicities, we state an assumption on 2-collisions (Assumption 4.3.8) under which we determine the root multiplicities of their components (Proposition 4.4.4). In Example 4.3.13 we see that the 2-collisions in Fact 4.2.1 and in Theorem 4.2.22 satisfy this assumption. Then we recall the well-known relation between decompositions of polynomials and towers of rational function fields. We reformulate a result by Dorey & Whaples (1974) about the ramification in such fields in the language of root multiplicities of polynomials (Proposition 4.3.23) and derive further properties about the multiplicities in collisions for which Assumption 4.3.8 holds.

We use the following notation. Let F be a field of characteristic $p > 0$ and $K = \overline{F}$ an algebraic closure of F. For a nonzero polynomial $f \in F[x]$ and $b \in K$, let $\mathrm{mult}_b(f)$ denote the *root multiplicity* of b in f, so that $f = (x-b)^{\mathrm{mult}_b(f)}u$ with $u \in K[x]$ and $u(b) \neq 0$. For $c \in K$, we denote as $f^{-1}(c)$ the set of all $b \in K$ such that $f(b) = c$.

Lemma 4.3.1. *Let* $f = g \circ h \in P_n(F)$ *and* $c \in K$. *Then*

$$f^{-1}(c) = \dot{\bigcup_{a \in g^{-1}(c)}} h^{-1}(a)$$

is a partition of $f^{-1}(c)$, *and for all* $b \in f^{-1}(c)$, *we have*

$$\mathrm{mult}_b(f-c) = \mathrm{mult}_{h(b)}(g-c) \cdot \mathrm{mult}_b(h-h(b)). \tag{4.3.2}$$

The partition of $f^{-1}(c)$ from Lemma 4.3.1 is illustrated in Figure 4.3.3, where we write $g^{-1}(c) = \{a_0, a_1, a_2, \dots\}$ and $h^{-1}(a_i) = \{a_{i0}, a_{i1}, a_{i2}, \dots\}$ for $i \geqslant 0$.

Proof. Let $b \in \bigcup_{a \in g^{-1}(c)} h^{-1}(a)$ and $a \in g^{-1}(c)$ such that $b \in h^{-1}(a)$. Hence $f(b) = g(h(b)) = g(a) = c$ and thus $b \in f^{-1}(c)$. On the other hand, let $b \in f^{-1}(c)$ and set $a = h(b)$. Then $b \in h^{-1}(a)$ and $a \in g^{-1}(c)$, since $g(a) = g(h(b)) = c$. Hence $b \in \bigcup_{a \in g^{-1}(c)} h^{-1}(a)$. Moreover if $b \in h^{-1}(a) \cap h^{-1}(a_0)$ for some a, $a_0 \in K$, then $a = h(b) = a_0$.

For (4.3.2), let $b \in f^{-1}(c)$, $a = h(b)$, $e = \mathrm{mult}_a(g-c)$, and $e_0 = \mathrm{mult}_b(h-a)$. Then $g - c = (x-a)^e G$ and $h - a = (x-b)^{e_0} H$ for some $G, H \in K[x]$ with $G(a) \cdot H(b) \neq 0$. Thus $f - c = g(h) - c = (h-a)^e G(h) = ((x-b)^{e_0} H)^e G(h) = (x-b)^{ee_0} H^e G(h)$ with $(H^e G(h))(b) = H(b)^e G(a) \neq 0$. □

Lemma 4.3.4. *Let* $f \in K[x]$ *and* $b \in K$. *Then* b *is a root of* f' *if and only if there is some* $c \in K$ *with* $\mathrm{mult}_b(f-c) > 1$. *Moreover, for any* $c \in K$ *with* $p \nmid \mathrm{mult}_b(f-c)$, *we have* $\mathrm{mult}_b(f') = \mathrm{mult}_b(f-c) - 1$.

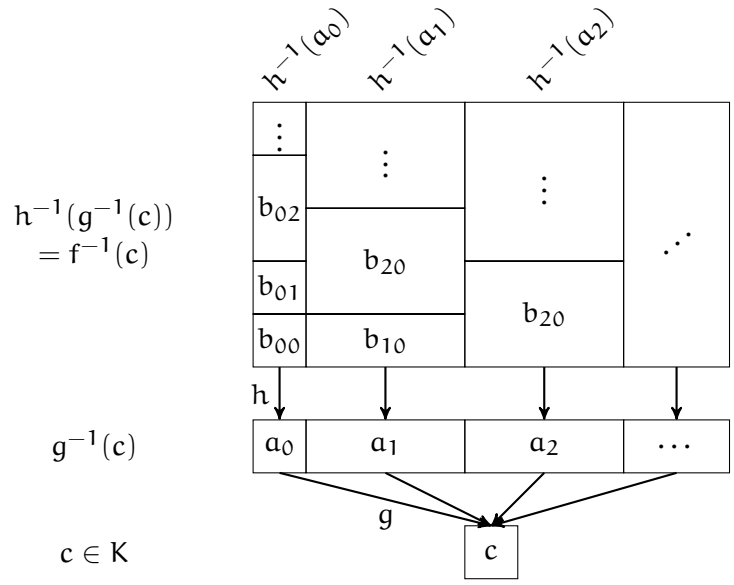

Figure 4.3.3: Partition of $f^{-1}(c)$

Proof. Let b be a root of f' and set $c = f(b)$. Then b is a root of $f - c$. We write $f - c = (x - b)u$ for some $u \in K[x]$. Then $f' = (f - c)' = u + (x - b)u'$, and thus $u(b) = f'(b) = 0$. Hence b is a multiple root of $f - c$.

Now, let $c \in K$ with $e = \operatorname{mult}_b(f - c)$. Then $f - c = (x - b)^e u$ for some $u \in K[x]$ with $u(b) \neq 0$ and $f' = (f - c)' = (x - b)^{e-1}(eu + (x - b)u')$. Thus, b is a root of f' if $e > 1$. This proves the converse. Moreover, if $p \nmid e$ then $(eu + (x - b)u')(b) = eu(b) \neq 0$ and hence $\operatorname{mult}_b(f') = e - 1$. □

We use the following proposition. The second part was stated as Proposition 6.5 (i) in von zur Gathen, Giesbrecht & Ziegler (2010) for $F = \mathbb{F}_q$.

Proposition 4.3.5. *Let r be a power of p and $f \in P_{r^2}(F)$ have a 2-collision C such that $\deg g = \deg h = r$ and $g'h' \neq 0$ for all $(g, h) \in C$. Then $f' \neq 0$ and the following hold.*

(i) There are integers d_1 and d_2 such that $\deg g' = d_1$ and $\deg h' = d_2$ for all $(g, h) \in C$.

(ii) Furthermore, if $r = p$, then $d_1 = d_2$.

Proof. (i) Let $(g, h) \in C$ and $f = g \circ h$. Then

$$\deg f' = \deg g' \cdot \deg h + \deg h'. \tag{4.3.6}$$

Since $g'h' \neq 0$, this is an equation of nonnegative integers. Moreover, $\deg h' < \deg h = r$ and thus $\deg g'$ and $\deg h'$ are uniquely determined by $\deg f'$ and r, which proves the claim.

(ii) For $r = p$, let $\ell = \deg_2 g$ and $m = \deg_2 h$ with the second degree $\deg_2$ as in (4.2.4). Since $g'h' \neq 0$, we find $d_1 = \deg g' = \ell - 1$ and $d_2 = \deg h' = m - 1$ for all $(g, h) \in C$ and it is sufficient to show $\ell = m$. We have

$$\begin{aligned} g &= x^p + g_\ell x^\ell + O(x^{\ell-1}), \\ h &= x^p + h_m x^m + O(x^{m-1}) \end{aligned}$$

with $g_\ell, h_m \in F^\times$. The highest terms in h^ℓ and $g \circ h$ are given by

$$\begin{aligned} h^\ell &= (x^p + h_m x^m + O(x^{m-1}))^\ell \\ &= x^{\ell p} + \ell h_m x^{(\ell-1)p+m} + O(x^{(\ell-1)p+m-1}), \\ g \circ h &= x^{p^2} + h_m^p x^{mp} + O(x^{(m-1)p}) + g_\ell x^{\ell p} + \ell g_\ell h_m x^{(\ell-1)p+m} \\ &\quad + O(x^{(\ell-1)p+m-1}) + O(x^{(\ell-1)p}). \end{aligned} \tag{4.3.7}$$

Algorithm 4.10 of von zur Gathen (2013) computes the components g and h from f, provided that $h_{p-1} \neq 0$. We do not assume this, but can apply the same method. Once g_ℓ and h_m are determined, the remaining coefficients first of h, then of g, are computed by solving linear equations of the form $uh_i = v$, where u and v are known at that point, and $u \neq 0$. Quite generally, g is determined by f and h, see Lemma 4.1.3.

For $(g^*, h^*) \in C$, we find that $(g_\ell, h_m) = (g_\ell^*, h_m^*)$ implies $(g, h) = (g^*, h^*)$ by the uniqueness of the procedure just sketched. Inspection of the coefficient of $x^{(\ell-1)p+m}$ in (4.3.7) shows that $g_\ell = g_\ell^*$ if and only if $h_m = h_m^*$.

Now take some $(g^*, h^*) \in C$ and assume that $\ell \neq m$. Then $\deg_2(g \circ h)$ is one of the two distinct integers mp or ℓp. If $m > \ell$, then h_m^p (and hence h_m) is uniquely determined by f, and otherwise g_ℓ is. In either case, we conclude from the previous observation that $(g, h) = (g^*, h^*)$. This shows $\ell = m$ if $(g, h) \neq (g^*, h^*)$. □

A *common right component* (over K) of two polynomials $h, h^* \in K[x]$ is a nonlinear polynomial $v \in K[x]$ such that $h = u \circ v$ and $h^* = u^* \circ v$ for some $u, u^* \in K[x]$. We now state an assumption which we use in Proposition 4.3.23, the lemmas thereafter, and in Proposition 4.4.4.

Assumption 4.3.8. Let $f \in P_n(F)$ have a 2-collision $\{(g, h), (g^*, h^*)\}$. We consider the following conditions.

(A_1) The derivative f' is nonzero.

(A_2) The degrees of all components are equal, that is, $\deg g = \deg g^* = \deg h = \deg h^*$.

(A_3) The right components h and h^* have no common right component over K.

(A_4) For all $c \in K$, neither $g - c$ nor $g^* - c$ have roots in K with multiplicity divisible by p.

(A_5) The degrees of g' and $h^{*\prime}$ are equal.

Lemma 4.3.9. *Let $f \in P_n(F)$ have a 2-collision $\{(g,h),(g^*,h^*)\}$.*

(i) Assumption (A_1) holds if and only if all derivatives g', $g^{*\prime}$, h', and $h^{*\prime}$ are nonzero.

(ii) If h or h^* is indecomposable, then (A_3) holds. In particular, it holds if $\deg h = \deg h^*$ is prime.

(iii) If $\deg g = p$ and (A_1) holds, then (A_4) holds.

(iv) If $n = p^2$ and (A_1) holds, then (A_5) holds.

(v) If (A_1), (A_2), and (A_5) hold, then $\deg g' = \deg g^{*\prime} = \deg h' = \deg h^{*\prime}$.

Proof. (i) The claim follows from the fact that $f' = g'(h) \cdot h'$.

(ii) Assume that h is indecomposable. Then a common right component of h and h^* would imply $h = h^*$ and thus $(g,h) = (g^*,h^*)$, by Lemma 4.1.3, a contradiction. Hence (A_3) holds. Moreover, polynomials of prime degree are indecomposable.

(iii) If a root multiplicity of $g - c$ was divisible by p for some $c \in K$, then $g - c = (x-a)^p$ for some $a \in K$. This would imply $g' = 0$, contradicting (A_1). Similarly, for all $c \in K$ the root multiplicities of $g^* - c$ are not divisible by p. Thus (A_4) holds.

(iv)–(v) We can apply Proposition 4.3.5, since $\deg g = \deg g^* = \deg h = \deg h^*$ by $n = p^2$ or (A_2), respectively, and $g'h'g^{*\prime}h^{*\prime} \neq 0$ by (A_1) and (i). Then (ii) of the cited proposition shows $\deg g' = \deg g^{*\prime} = \deg h' = \deg h^{*\prime}$, proving (iv) and (v). □

In Example 4.3.13 we show that Assumption 4.3.8 holds for the collisions in Fact 4.2.1 and in Theorem 4.2.22. We need the next two propositions to check (A_3) for these collisions.

Proposition 4.3.10. *Let r be a power of p, let $a, a^* \in F$ and m be a positive divisor of $r-1$, $\ell = (r-1)/m$, and*

$$h = x(x^\ell - a)^m,$$
$$h^* = x(x^\ell - a^*)^m.$$

If h and h^* have a common right component, then $h = h^*$. In particular, the right components in 2-collisions of the form as in Fact 4.2.1 have no common right component.

Proof. By Henderson & Matthews (1999, Theorem 4.1) it suffices to prove the claim for additive polynomials, that is, for $m = 1$. Furthermore, we can assume without loss of generality that F is algebraically

closed. Let $v \in P_{p^\nu}(F)$ be a common right component of h and h^* with $h = u \circ v$ and $h^* = u^* \circ v$ for some $u, u^* \in P_{p^k}(F)$, $\nu \geqslant 1$, and $r = p^{k+\nu}$. Then u, u^*, and v are additive polynomials; see Cohen (1990b, Lemma 2.4). By Ore (1933, Theorem 3 in Chapter 1) and since F is algebraically closed, we may assume $v = 1$ and $v = x^p - bx$, for some $b \in F$. For $u = \sum_{0 \leqslant i \leqslant k} u_i x^{p^i}$, we have

$$\begin{aligned} h = x^r - ax &= u \circ (x^p - bx) \\ &= u_k x^r + \sum_{1 \leqslant i \leqslant k} (u_{i-1} - u_i b^{p^i}) x^{p^i} - u_0 bx. \end{aligned}$$

Thus $u_k = 1$ and $u_{i-1} = u_i b^{p^i} = \prod_{i \leqslant j \leqslant k} b^{p^j}$, for $1 \leqslant i \leqslant k$. Moreover, $a = u_0 b = \prod_{0 \leqslant j \leqslant k} b^{p^j}$ is uniquely determined by b. Thus $a = a^*$ and $h = h^*$. □

Proposition 4.3.11. *Let* r, b, a, a^*, m, m^*, g, *and* h *be as in Theorem 4.2.22. Then* g *and* h *are indecomposable.*

Proof. Let $g = u \circ v$ with $u \in P_k(F)$, $v \in P_\ell(F)$, $k\ell = r$, and $\ell > 1$. Then $p \mid \ell$. By Lemma 4.3.1 we have

$$\dot{\bigcup_{a_0 \in u^{-1}(0)}} v^{-1}(a_0) = g^{-1}(0) = \{0, a\}. \tag{4.3.12}$$

Since v is original, we have $\{0\} \subseteq v^{-1}(0) \subseteq \{0, a\}$. If $v^{-1}(0) = \{0\}$, then $v = x^\ell$ and thus $p \mid \ell \mid m$, by (4.3.2), in contradiction to $p \nmid m$. Thus $v^{-1}(0) = \{0, a\}$. Since the union in (4.3.12) is disjoint, we find that $u^{-1}(0) = \{0\}$ and 0 is the only root of u. Hence $u = x^k$ and $k \mid \gcd(m, m^*) = 1$, by (4.3.2) and Proposition 4.2.26 (i). Therefore u is linear and thus g is indecomposable.

By (4.2.24) and Proposition 4.2.26 (i), we find $h = x^{m^*} H$ and $h - a = (x-b)^m H^*$ with squarefree polynomials H and H^*. Thus $h^{[b]} = x^m \tilde{H}$ for squarefree $\tilde{H} = H^* \circ (x + b)$. We find that h is decomposable if and only if $h^{[b]}$ is decomposable. By Proposition 4.2.26 (iii) either $m > r/2$ or $m^* > r/2$. If $m > r/2$, then we rename h as $h^{[b]}$, H as $\tilde{H}$ and m as m^*. We have in either case $m^* > r/2$.

Now let $h = u \circ v$ with $u \in P_k(F)$, $v \in P_\ell(F)$, $k\ell = r$, and $\ell > 1$. Then $p \mid \ell$. The only multiple root in h is 0, since H is squarefree, by Proposition 4.2.26 (i). Its multiplicity is $\mathrm{mult}_0(h) = m^* = \mathrm{mult}_0(u) \cdot \mathrm{mult}_0(v)$. Thus $\mathrm{mult}_0(v) \mid m^*$ and hence $p \nmid \mathrm{mult}_0(v)$. Since the multiplicities of v sum up to ℓ, which is divisible by p, there is another root $b_0 \neq 0$ of v. Then $1 = \mathrm{mult}_{b_0}(h) = \mathrm{mult}_0(u) \cdot \mathrm{mult}_{b_0}(v)$ and thus $\mathrm{mult}_0(u) = 1$. Hence $\mathrm{mult}_0(v) = m^*$. We have $\ell > m^* > r/2$, thus $\ell = r$ and u is linear. □

Example 4.3.13. Assumption 4.3.8 holds for the #T-collisions in Fact 4.2.1 with $\#T \geqslant 2$ and the 2-collisions in Theorem 4.2.22. In both cases (A_2)

holds by definition. Assumption (A_3) follows from Proposition 4.3.10 and from Proposition 4.3.11 and Lemma 4.3.9 (ii), respectively.

The derivatives of the components in Fact 4.2.1 are

$$\begin{aligned} g' &= -us^r t^{-1}(x^\ell - us^r t^{-1})^{m-1}, \\ h' &= -st(x^\ell - st)^{m-1}. \end{aligned} \tag{4.3.14}$$

Since u, s, $t \in F^\times$, we find $\deg g' = \deg h' = \ell(m-1) \geqslant 0$, independent of $t \in T$, and thus (A_5) holds. By (4.3.6), $\deg f' \geqslant 0$ and thus (A_1) holds. If there is $c \in K$ such that $g - c$ has a multiple root $b \in K$, then b is also a root of g' by Lemma 4.3.4. Since $g'^{-1}(0) \subseteq g^{-1}(0)$ by (4.3.14), we have only simple roots in $g - c$ for $c \neq 0$. The multiple roots of g have multiplicity m and (A_4) follows from $p \nmid m \mid r - 1$.

For the collisions in Theorem 4.2.22, (A_4) follows similarly from $p \nmid mm^*$. Finally, (A_1) and (A_5) are satisfied by (4.2.27) and a, a^*, $b \in F^\times$.

Lemma 4.3.15. *Let $f \in F[x]$ be monic and y be transcendental over $K(x)$. Then $f - y \in K(y)[x]$ is irreducible.*

Proof. Assume $f - y = uv$ for some $u, v \in K[x, y]$. The degree in y of $f - y$ is $\deg_y(f - y) = 1 = \deg_y u + \deg_y v$. Thus we may assume $\deg_y u = 1$ and $\deg_y v = 0$. Then $av = -1$, where $a \in K[x]$ is the leading coefficient of u in y. Thus $v \in K[x]^\times = K^\times$ and $f - y$ is irreducible in $K[x, y]$. A factorization of $f - y$ in $K(y)[x]$ yields a factorization in $K[x, y]$, by the Lemma of Gauß, see Lang (2002, Corollary 2.2 in Capter IV). Hence $f - y$ is also irreducible in $K(y)[x]$. □

Let $f \in P_n(F)$ with $f' \neq 0$ and y be transcendental over $K(x)$. Then $f - y \in K(y)[x]$ is irreducible and separable over $K(y)$, by Lemma 4.3.15 and since the derivative of $f - y$ with respect to x is $(f - y)' = f' \neq 0$. In particular, $f - y \in F(y)[x]$ is irreducible and separable. Let $\alpha \in \overline{K(y)}$ be a root of $f - y$. Then $K(y)[\alpha] = K(\alpha)$ is a rational extension of $K(y)$ of degree n. Let $\mathcal{M}$ be the set of intermediate fields between $K(\alpha)$ and $K(y)$ and $\mathcal{R} = \{h \in P_m(K) \colon m \mid n \text{ and there is } g \in P_{n/m}(K) \text{ such that } f = g \circ h\}$ be the set of right components of f.

Fact 4.3.16 (Fried & MacRae (1969), Proposition 3.4)**.** *Let $f \in P_n(K)$ with $f' \neq 0$ and let $\alpha \in \overline{K(y)}$ be a root of $f - y \in K(y)[x]$. Then the map*

$$\begin{aligned} &\mathcal{R} \to \mathcal{M}, \\ &h \mapsto K(h(\alpha)) \end{aligned} \tag{4.3.17}$$

is bijective.

The fact follows from Fried & MacRae (1969, Proposition 3.4). Indeed, for each $u \in K[x]$ of degree m there is exactly one $v \in P_m(K)$ such that $u = \ell \circ v$ for some linear polynomial $\ell \in K[x]$; see von zur Gathen (2013, Section 2).

The sets $\mathcal{R}$ and $\mathcal{M}$ can be equipped with natural lattice structures for which (4.3.17) is an isomorphism.

We now use the theory of places and ramification indices in function fields; see Stichtenoth (2009) for the background. A *place* in a function field L over K is the maximal ideal of some valuation ring of L over K. For an finite extension M of L a place $\mathfrak{p}$ in M is said to lie over a place P in L if $P \subseteq \mathfrak{p}$. Then we write $\mathfrak{p} \mid P$ and define the ramification index of $\mathfrak{p} \mid P$ as the integer $e(\mathfrak{p} \mid P)$ such that $\nu_{\mathfrak{p}}(a) = e(\mathfrak{p} \mid P) \cdot \nu_P(a)$ for all $a \in L$, where $\nu_{\mathfrak{p}}$ and ν_P are the corresponding valuations of $\mathfrak{p}$ and P, respectively; see Stichtenoth (2009, Proposition 3.1.4 and Definition 3.1.5).

Later, we translate this into the language of root multiplicities of polynomials. First, we need the following result, which is proven in Dorey & Whaples (1974, Lemma 1) for rational function fields under the assumption that the characteristic of K is zero. Our proof avoids this assumption.

Theorem 4.3.18. *Let* L, M, M^*, N *be function fields over* K *such that* $L \subseteq M, M^* \subseteq N$ *are finite separable field extensions and* $M \otimes_L M^* \cong MM^* = N$. *Let* P *be a place in* L, *and* $\mathfrak{p}$, $\mathfrak{p}^*$ *be places over* P *in* M *and* M^*, *respectively. Assume that at least one of the ramification indices* $m = e(\mathfrak{p} \mid P)$ *and* $m^* = e(\mathfrak{p}^* \mid P)$ *is not divisible by the characteristic of* K. *Then there are* $\gcd(m, m^*)$ *places* $\mathfrak{q}$ *in* N *which lie over* $\mathfrak{p}$ *and over* $\mathfrak{p}^*$. *Moreover, for such a place we have* $e(\mathfrak{q} \mid P) = \operatorname{lcm}(m, m^*)$.

Proof. Abhyankar's Lemma says that for a place $\mathfrak{q}$ in N over $\mathfrak{p}$ and over $\mathfrak{p}^*$,

$$e(\mathfrak{q} \mid P) = \operatorname{lcm}(m, m^*), \tag{4.3.19}$$

see Stichtenoth (2009, Theorem 3.9.1). Now we proceed as in Dorey & Whaples (1974). For places $\mathfrak{p}$, $\mathfrak{p}^*$, and $\mathfrak{q}$ over P in M, M^*, and N, respectively, we denote by $\Lambda = \widehat{L}$, $\widehat{M}^{\mathfrak{p}}$, $\widehat{M^*}^{\mathfrak{p}^*}$, and $\widehat{N}^{\mathfrak{q}}$ the completions of L, M, M^*, and N with respect to P, $\mathfrak{p}$, $\mathfrak{p}^*$, and $\mathfrak{q}$, respectively. The tensor product $N \otimes_M \widehat{M}^{\mathfrak{p}}$ is the direct sum of the completions of N with respect to the places in N over $\mathfrak{p}$, and $M^* \otimes_L \Lambda$ is the direct sum of the completions of M^* with respect to the places in M^* over P; see Neukirch (1999, Proposition 8.3 in Chapter II). Since $M \otimes_L M^* \cong N$, we have

$$\begin{aligned}\bigoplus_{\mathfrak{q} \mid \mathfrak{p}} \widehat{N}^{\mathfrak{q}} &\cong N \otimes_M \widehat{M}^{\mathfrak{p}} \cong M^* \otimes_L M \otimes_M \widehat{M}^{\mathfrak{p}} \cong M^* \otimes_L \widehat{M}^{\mathfrak{p}} \\ &\cong M^* \otimes_L (\Lambda \otimes_\Lambda \widehat{M}^{\mathfrak{p}}) \cong (M^* \otimes_L \Lambda) \otimes_\Lambda \widehat{M}^{\mathfrak{p}} \\ &\cong \bigoplus_{\mathfrak{p}_0^* \mid P} \widehat{M^*}^{\mathfrak{p}_0^*} \otimes_\Lambda \widehat{M}^{\mathfrak{p}},\end{aligned}$$

where the last direct sum is taken over all places $\mathfrak{p}_0^*$ in M^* over P. We show that $\widehat{M^*}^{\mathfrak{p}^*} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$ is the direct sum of the completions of N with respect to the places that lie over $\mathfrak{p}$ and $\mathfrak{p}^*$. For this purpose, consider

the (external) composite fields of $\widehat{M^{*\mathfrak{p}^*}}$ and $\widehat{M}^{\mathfrak{p}}$ in an algebraic closure Ω of $\widehat{N}^{\mathfrak{q}}$; those are the field extensions $\Gamma \subseteq \Omega$ of Λ such that there are two field homomorphisms which map $\widehat{M^{*\mathfrak{p}^*}}$ and $\widehat{M}^{\mathfrak{p}}$, respectively, into Γ and whose images generate Γ. Then $\widehat{M^{*\mathfrak{p}^*}} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$ is the direct sum of the composite fields of $\widehat{M^{*\mathfrak{p}^*}}$ and $\widehat{M}^{\mathfrak{p}}$; see Jacobson (1964, Theorem 21 in Chapter I). Each such composite field Γ is isomorphic to a summand in $\bigoplus_{\mathfrak{q}|\mathfrak{p}} \widehat{N}^{\mathfrak{q}}$, by the Krull-Remak-Schmidt Theorem; see Lang (2002, Theorem 7.5). Thus there exists $\mathfrak{q} \mid \mathfrak{p}$ such that $\Gamma = \widehat{N}^{\mathfrak{q}}$. Since Γ is an extension of $\widehat{M^{*\mathfrak{p}^*}}$, we find $\mathfrak{q} \mid \mathfrak{p}^*$ as claimed. On the other hand, for a place $\mathfrak{q}$ in N over $\mathfrak{p}$ and $\mathfrak{p}^*$, $\widehat{N}^{\mathfrak{q}}$ is a composite field of $\widehat{M^{*\mathfrak{p}^*}}$ and $\widehat{M}^{\mathfrak{p}}$ and thus is a summand in $\widehat{M^{*\mathfrak{p}^*}} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$.

The summands of $\widehat{M^{*\mathfrak{p}^*}} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$ are of degree $\operatorname{lcm}(m, m^*)$, by (4.3.19), and the Λ-dimension of $\widehat{M^{*\mathfrak{p}^*}} \otimes_\Lambda \widehat{M}^{\mathfrak{p}}$ is mm^*. Thus there are $mm^*/\operatorname{lcm}(m, m^*) = \gcd(m, m^*)$ places over $\mathfrak{p}$ and $\mathfrak{p}^*$. □

In the following we link the notion of places and ramification indices to the notion of roots and root multiplicities. Let $K(t)$ be a rational function field. Then the local ring $\mathcal{O}_\infty = \{g/h \in K(t) \colon g, h \in K[t], \deg g \leqslant \deg h\}$ is the $1/t$-adic valuation ring of $K(t)$ and $P_\infty = (1/t)\mathcal{O}_\infty$ is its maximal ideal. For $c \in K$, the local ring $\mathcal{O}_{t-c} = \{g/h \in K(t) \colon g, h \in K[t], h(c) \neq 0\}$ is the $(t-c)$-adic valuation ring of $K(t)$ and $P_c = (t-c)\mathcal{O}_{t-c}$ is its maximal ideal. We denote the $(t-c)$-adic valuation by v_{P_c}. Then we have for $f \in K[x]$

$$v_{P_c}(f(t)) = \operatorname{mult}_c(f). \tag{4.3.20}$$

Since the irreducible polynomials in $K[t]$ are linear, the places P_∞ and P_c for all $c \in K$ are pairwise distinct and comprise all places in $K(t)$; see Stichtenoth (2009, Theorem 1.2.2). We call the places P_c *finite* places. The map

$$\begin{aligned} K &\to \{P \colon P \text{ is a finite place in } K(t)\}, \\ c &\mapsto P_c \end{aligned} \tag{4.3.21}$$

is bijective.

Lemma 4.3.22. *Let $f \in P_n(K)$ with $f' \neq 0$, let $\alpha \in \overline{K(y)}$ be a root of $f - y \in K(y)[x]$, let $b, c \in K$, and let P_c and $\mathfrak{q}_b$ be the corresponding finite places in $K(y)$ and $K(\alpha)$, respectively. Then $\mathfrak{q}_b \mid P_c$ if and only if $f(b) = c$. Furthermore*

$$e(\mathfrak{q}_b \mid P_c) = \operatorname{mult}_b(f - c).$$

Proof. Let $\mathfrak{q}_b \mid P_c$. Then $y - c \in \mathfrak{q}_b$ and thus $f(\alpha) - c = y - c = (\alpha - b)g/h$ for $g, h \in K[\alpha]$ with $h(b) \neq 0$. Hence, $f(b) - c = (b - b)g(b)/h(b) = 0$.

Conversely, let $f(b) = c$. Then $\alpha - b \mid f(\alpha) - c$ in $K[\alpha]$. Let $(y - c)g/h \in P_c$ for some $g, h \in K[y]$ with $h(c) \neq 0$. Then $h(f(b)) = h(c) \neq 0$ and thus $(y - c)g/h = (f(\alpha) - c)g(f(\alpha))/h(f(\alpha)) \in \mathfrak{q}_b$.

By (4.3.20) and since $v_{P_c}(y-c)=1$, we have $e(q_b \mid P_c) = v_{q_b}(y-c) = v_{q_b}(f(\alpha)-c) = \operatorname{mult}_b(f-c)$. □

Proposition 4.3.23. *Let* $c \in K$ *and* $f \in P_n(F)$ *have a 2-collision* $\{(g,h), (g^*,h^*)\}$ *satisfying* (A_1)–(A_4) *in Assumption 4.3.8. For* $a \in g^{-1}(c)$ *and* $a^* \in g^{*-1}(c)$, *there are exactly* $\gcd(\operatorname{mult}_a(g-c), \operatorname{mult}_{a^*}(g^*-c))$ *roots* $b \in f^{-1}(c)$ *such that* $h(b)=a$ *and* $h^*(b)=a^*$. *Furthermore, for each such root* b *we have*

$$\operatorname{mult}_b(f-c) = \operatorname{lcm}(\operatorname{mult}_a(g-c), \operatorname{mult}_{a^*}(g^*-c)). \tag{4.3.24}$$

Proof. By (A_1) we have $f' \neq 0$ and thus $f-y \in F(y)[x]$ is irreducible and separable; see Lemma 4.3.15 and the paragraph thereafter. Let $\alpha \in \overline{K(y)}$ be a root of $f-y$, $M = K(h(\alpha))$ and $M^* = K(h^*(\alpha))$, as in (4.3.17). Then α is a root of $h-h(\alpha)$ and by Lemma 4.3.15, $h-h(\alpha)$ is irreducible in $M[x]$. Thus the minimal polynomial of α over M is $h-h(\alpha)$, and similarly the minimal polynomial of $h(\alpha)$ over $K(y)$ is $g-y$. Hence $[K(\alpha)\colon M] = \deg h$ and $[M\colon K(y)] = \deg g$. Figure 4.3.25 illustrates the relation between these field extensions and their respective minimal polynomials.

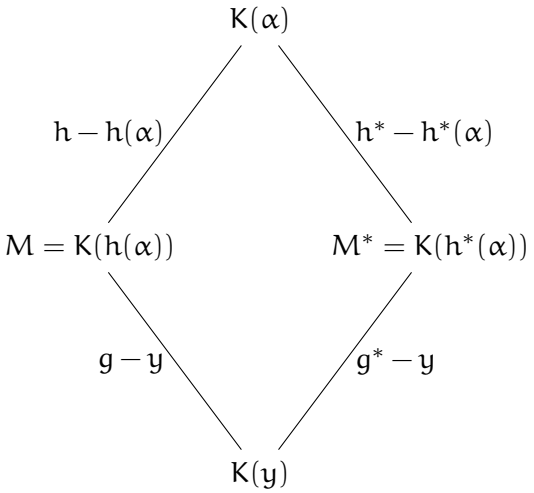

Figure 4.3.25: Lattice of subfields

By Fact 4.3.16 and since $MM^* \subseteq K(\alpha)$, there is a monic original $v \in K[x]$ such that $MM^* = K(v(\alpha))$. Since $M \subseteq MM^*$, there is $u \in K[x]$ such that $h = u \circ v$, by applying Fact 4.3.16 to $K(\alpha) \mid M$. Similarly, there is $u^* \in K[x]$ such that $h^* = u^* \circ v$. Hence $v = x$, by (A_3), and $MM^* = K(\alpha)$. Moreover, MM^* is contained in $M \otimes_{K(y)} M^*$ as a direct summand; see Jacobson (1964, Theorem 21 in Chapter I). Their $K(y)$-dimensions both equal $\deg f = \deg g \cdot \deg h = (\deg g)^2$, by (A_2). Thus $M \otimes_{K(y)} M^* \cong MM^* = K(\alpha)$. Let P_c be as in (4.3.21). Since, by Lemma 4.3.22, the root multiplicities of $g-c$ are the ramification indices of the places over P_c in M, (A_4) rules out finite wildly ramified places in $M \mid K(y)$. Thus we can apply Theorem 4.3.18, as follows.

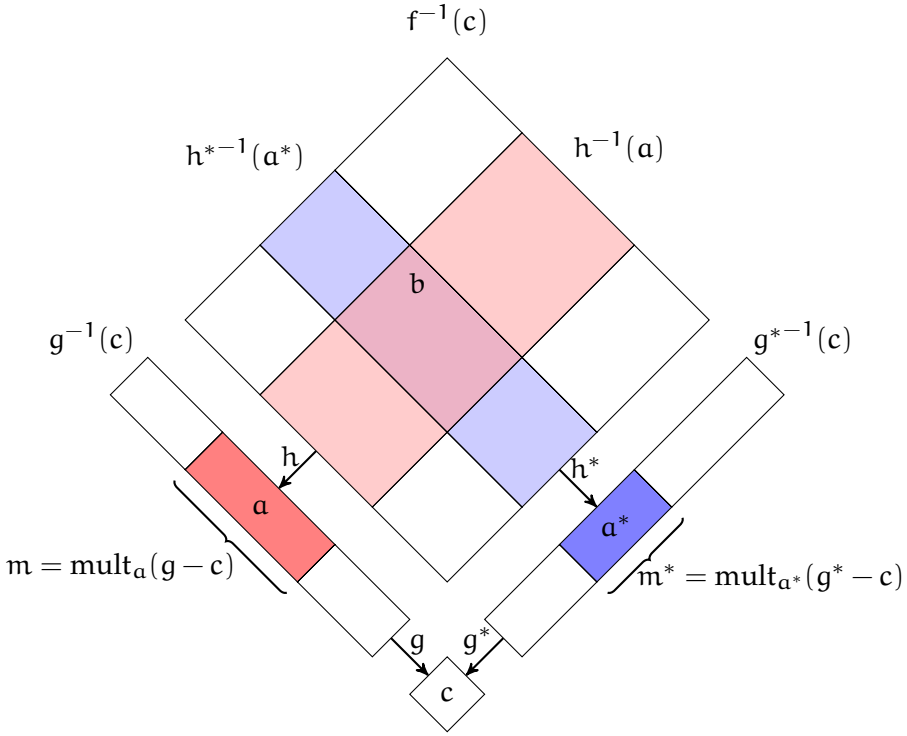

Figure 4.3.26: Roots and multiplicities

Let $m = \mathrm{mult}_a(g-c)$ and $m^* = \mathrm{mult}_{a^*}(g^*-c)$, see Figure 4.3.26. By Lemma 4.3.22, there are finite places $\mathfrak{p}_a$ and $\mathfrak{p}^*_{a^*}$ over P_c in M and M^*, respectively, with $m = e(\mathfrak{p}_a \mid P_c)$ and $m^* = e(\mathfrak{p}^*_{a^*} \mid P_c)$. Then, by Theorem 4.3.18, there are $\gcd(m, m^*)$ places $\mathfrak{q}$ over $\mathfrak{p}_a$ and $\mathfrak{p}^*_{a^*}$ in $K(\alpha)$. By the bijection (4.3.21), for each such place $\mathfrak{q}$ there is $b \in K$ such that $\mathfrak{q} = \mathfrak{q}_b$, and by applying Lemma 4.3.22 to $K(\alpha) \mid M$ and to $K(\alpha) \mid M^*$, we find $b \in h^{-1}(a) \cap h^{*-1}(a^*) \subseteq f^{-1}(c)$. On the other hand, for $b \in h^{-1}(a) \cap h^{*-1}(a^*)$, the place $\mathfrak{q}_b$ lies over $\mathfrak{p}_a$ and $\mathfrak{p}^*_{a^*}$. Thus $\#h^{-1}(a) \cap h^{*-1}(a^*) = \gcd(m, m^*)$ and $\mathrm{mult}_b(f-c) = e(\mathfrak{q}_b \mid P_c) = \mathrm{lcm}(m, m^*)$, by Theorem 4.3.18. □

Combining (4.3.24) and (4.3.2), for $b \in K$, $a = h(b)$, $a^* = h^*(b)$, and $c = f(b)$, we find $\mathrm{mult}_a(g-c) \cdot \mathrm{mult}_b(h-a) = \mathrm{mult}_b(f-c) = \mathrm{lcm}\,(\mathrm{mult}_a(g-c), \mathrm{mult}_{a^*}(g^*-c))$ and thus

$$\mathrm{mult}_b(h-a) = \mathrm{lcm}\,(\mathrm{mult}_a(g-c), \mathrm{mult}_{a^*}(g^*-c)) \,/\, \mathrm{mult}_a(g-c). \tag{4.3.27}$$

Hence, the root multiplicities of $h-a$ are determined by those of $g-c$ and g^*-c.

From Proposition 4.3.23 we derive further results about the root multiplicities of f, g, and g^*.

Lemma 4.3.28. *Let $c \in K$, r be a power of p, $f \in P_{r^2}(F)$ have a 2-collision $\{(g,h),(g^*,h^*)\}$ satisfying Assumption 4.3.8, and let $a \in g^{-1}(c)$ and $e = \mathrm{mult}_a(g-c)$. Then the following hold.*

(i) We have

$$\gcd\{\mathrm{mult}_{a^*}(g^* - c)\colon a^* \in {g^*}^{-1}(c)\} = 1. \tag{4.3.29}$$

In particular, if e *divides* $\mathrm{mult}_{a^*}(g^* - c)$ *for all roots* $a^* \in {g^*}^{-1}(c)$*, then* $e = 1$*.*

(ii) The multiplicity e *either equals* 1 *or divides* $\mathrm{mult}_{a^*}(g^* - c)$ *for all roots* $a^* \in {g^*}^{-1}(c)$ *but exactly one.*

Proof. (i) Let d be the gcd of all root multiplicities of $g^* - c$. Then d divides $\sum_{a^* \in {g^*}^{-1}(c)} \mathrm{mult}_{a^*}(g^* - c) = \deg(g^* - c) = r$. Thus d is a power of p and hence all multiplicities of $g^* - c$ are divisible by p if $d > 1$, which contradicts (A_4), and (i) follows.

Before we start with the proof of (ii), we introduce some notation and results for arbitrary $c \in K$, $a \in g^{-1}(c)$, and $a^* \in {g^*}^{-1}(c)$. We define

$$\begin{aligned} i(c, g) &= \sum_{a \in g^{-1}(c)} \mathrm{mult}_a(g'), \\ i(c, h^*) &= \sum_{b \in f^{-1}(c)} \mathrm{mult}_b(h^{*\prime}), \\ j(a, a^*) &= \sum_{b \in h^{-1}(a) \cap {h^*}^{-1}(a^*)} \mathrm{mult}_b(h^{*\prime}), \end{aligned} \tag{4.3.30}$$

and have

$$\begin{aligned} \sum_{c \in K} i(c, g) &= \deg g', \\ \sum_{c \in K} i(c, h^*) &= \deg h^{*\prime}, \\ \sum_{\substack{a \in g^{-1}(c) \\ a^* \in {g^*}^{-1}(c)}} j(a, a^*) &= i(c, h^*), \end{aligned} \tag{4.3.31}$$

since $\dot{\bigcup}_{c \in K} g^{-1}(c) = K$, $\dot{\bigcup}_{c \in K} f^{-1}(c) = K$, and

$$f^{-1}(c) = \dot{\bigcup_{\substack{a \in g^{-1}(c) \\ a^* \in {g^*}^{-1}(c)}}} h^{-1}(a) \cap {h^*}^{-1}(a^*)$$

by Lemma 4.3.1.

By (A_4), $p \nmid \mathrm{mult}_a(g - c)$ and thus $\mathrm{mult}_a(g') = \mathrm{mult}_a(g - c) - 1$, by Lemma 4.3.4. Hence for $c \in K$ we have

$$i(c, g) = \sum_{a \in g^{-1}(c)} (\mathrm{mult}_a(g - c) - 1) = \deg g - \#g^{-1}(c). \tag{4.3.32}$$

Let $e = \mathrm{mult}_a(g - c)$ and $e^* = \mathrm{mult}_{a^*}(g^* - c)$. By Proposition 4.3.23, the set $h^{-1}(a) \cap {h^*}^{-1}(a^*)$ has size $\gcd(e, e^*)$ and for a root $b \in$

$h^{-1}(a) \cap h^{*-1}(a^*)$, we have $\mathrm{mult}_b(h^* - a^*) = \mathrm{mult}_b(f - c)/e^* = \mathrm{lcm}(e, e^*)/e^*$, by (4.3.27). Thus $\mathrm{mult}_b(h^{*\prime}) = \mathrm{lcm}(e, e^*)/e^* - 1$ by (A_4) and Lemma 4.3.4 and we have

$$j(a, a^*) = \gcd(e, e^*) \cdot (\mathrm{lcm}(e, e^*)/e^* - 1) = e - \gcd(e, e^*). \quad (4.3.33)$$

We now show

$$\sum_{a^* \in g^{*-1}(c)} j(a, a^*) \geqslant e - 1. \quad (4.3.34)$$

Let $a_0^*, \ldots, a_\ell^*$ be the roots of $g^* - c$ in K and $e_i^* = \mathrm{mult}_{a_i^*}(g^* - c)$ be their multiplicities. If e divides all e_i^*, then $e = 1$ by (i) and (4.3.34) follows trivially. If e divides all e_i^* except exactly one, say $e \nmid e_0^*$ and $e \mid e_i^*$ for $1 \leqslant i \leqslant \ell$, then the gcd of e and e_0^* divides all e_i^* and hence divides $\gcd\{e_i^* \colon 0 \leqslant i \leqslant \ell\} = 1$; see (4.3.29). Thus $\gcd(e, e_0^*) = 1$, $j(a, a_0^*) = e - 1$ by (4.3.33), and (4.3.34) follows.

Now assume that e does not divide at least two e_i^*, say $e \nmid e_0^*$ and $e \nmid e_1^*$. Then $\gcd(e, e_i^*) \neq e$, $\gcd(e, e_i^*) \leqslant e/2$, and $j(a, a_i^*) \geqslant e/2$ by (4.3.33) for $i = 0, 1$. Hence, (4.3.34) holds with strict inequality. Summing both sides of (4.3.34) over all roots of $g - c$ yields

$$i(c, h^*) = \sum_{\substack{a \in g^{-1}(c) \\ a^* \in g^{*-1}(c)}} j(a, a^*) > \sum_{a \in g^{-1}(c)} (\mathrm{mult}_a(g - c) - 1) = i(c, g)$$

by (4.3.30) and (4.3.32). With (4.3.31), this leads to

$$\deg h^{*\prime} > \deg g',$$

a contradiction to (A_5). □

Lemma 4.3.35. *Let $c \in K$, r be a power of p, and let $f \in P_{r^2}(F)$ have a 2-collision $\{(g, h), (g^*, h^*)\}$ satisfying Assumption 4.3.8. Then the following statements are equivalent.*

(i) $g - c$ *is squareful.*

(ii) $g^* - c$ *is squareful.*

(iii) $f - c$ *is squareful.*

Furthermore, if $g - c$ is squareful, then $g - c$ has at most one simple root.

Proof. Assume that $g - c$ is squareful. Then there is a root of $g - c$ with multiplicity greater than 1. This multiplicity divides all multiplicities of $g^* - c$ but exactly one, by Lemma 4.3.28 (ii). Hence all multiplicities of $g^* - c$ but at most one are greater than 1. Thus $g^* - c$ is squareful and has at most one simple root. We interchange the rôles of g and g^* in Lemma 4.3.28 and obtain the equivalence of (i) and (ii) and the last claim.

Now let $a \in K$ be a multiple root of $g - c$, and $b \in h^{-1}(a)$. Then $\mathrm{mult}_b(f - c) = \mathrm{mult}_a(g - c) \cdot \mathrm{mult}_b(h - h(b)) > 1$, by Lemma 4.3.1, and thus $f - c$ is squareful.

It is left to prove that if $f - c$ is squareful, then $g - c$ or $g^* - c$ is squareful. Let $b \in K$ be a multiple root of $f - c$. Then $1 < \mathrm{mult}_b(f - c) = \mathrm{lcm}(\mathrm{mult}_{h(b)}(g - c), \mathrm{mult}_{h^*(b)}(g^* - c))$, by Proposition 4.3.23. Thus $\mathrm{mult}_{h(b)}(g - c) > 1$ or $\mathrm{mult}_{h^*(b)}(g^* - c) > 1$. □

Lemma 4.3.36. *Let r be a power of p, and let $f \in P_{r^2}(F)$ have a 2-collision $\{(g, h), (g^*, h^*)\}$ satisfying Assumption 4.3.8. Then the following hold.*

(i) There is at most one $c \in K$ such that $f - c$ is squareful.

(ii) For all $c \in K$, $\#g^{-1}(c) = \#g^{*-1}(c)$.

Proof. (i) Assume $g - c$ is squareful, for some $c \in K$. Then $g - c$ has at most one simple root, by Lemma 4.3.35. Thus $r = \deg g = \sum_{a \in g^{-1}(c)} \mathrm{mult}_a(g - c) \geqslant 1 + 2(\#g^{-1}(c) - 1)$. Hence $\#g^{-1}(c) \leqslant (r + 1)/2$ and thus $i(c, g) = r - \#g^{-1}(c) \geqslant (r - 1)/2$, by (4.3.32). Now, if there is another value $c_0 \in K \setminus \{c\}$ such that $g - c_0$ is also squareful, then $r - 2 \geqslant \deg g' = \sum_{c \in K} i(c, g) \geqslant r - 1$, by (4.3.31). By this contradiction, there is at most one c in K such that $g - c$ is squareful. Hence there is at most one c in K such that $f - c$ is squareful, by Lemma 4.3.35.

(ii) If $g - c$ is squarefree, then so is $g^* - c$, by Lemma 4.3.35, and both have exactly $\deg g = \deg g^* = r$ roots. If $g - c$ is squareful, then by (i), c is unique with this property and thus the roots of g' are the multiple roots of $g - c$ by Lemma 4.3.4. Hence

$$\deg g' = \mathrm{mult}_{a \in g^{-1}(c)} \mathrm{mult}_a(g') = i(c, g) = \deg g - \#g^{-1}(c) \tag{4.3.37}$$

by (4.3.32). Interchanging the rôles of g and g^* shows $\deg g^{*\prime} = \deg g^* - \#g^{*-1}(c)$ and Lemma 4.3.9 (v) yields $\deg g' = \deg g^{*\prime}$, thus $\#g^{-1}(c) = \#g^{*-1}(c)$. □

The previous lemmas deal with the root multiplicities over K. The next lemma shows that certain parameters are in F, when F is assumed to be perfect.

Lemma 4.3.38. *Let F be perfect, $c \in K$, r be a power of p, and $f \in P_{r^2}(F)$ have a 2-collision $\{(g, h), (g^*, h^*)\}$ satisfying Assumption 4.3.8. Then the following hold.*

(i) If $f - c$ is squareful, then $c \in F$.

(ii) If $g - c = g_1^{m_1} g_2^{m_2}$ for some monic squarefree coprime polynomials $g_1, g_2 \in K[x]$ and integers $m_1 \neq m_2$, then $c \in F$ and $g_1, g_2 \in F[x]$.

(iii) If $a \in F$ and $h - a = h_1^{m_1} h_2^{m_2}$ for some monic squarefree coprime polynomials $h_1, h_2 \in K[x]$ and positive integers $m_1 \neq m_2$, then $h_1, h_2 \in F[x]$.

Proof. Since F is perfect, K is Galois over F. An element $c \in K$ is fixed by all automorphisms in the Galois group $\mathrm{Gal}(K \mid F)$ if and only if $c \in F$.

(i) Let $f - c$ be squareful and $\sigma \in \mathrm{Gal}(K \mid F)$. Then $\sigma(f - c) = f - \sigma(c)$ is squareful as well. Indeed, if $f - c = (x - a)^2 u$ for some $a \in K$ and $u \in K[x]$, then $\sigma(f - c) = (x - \sigma a)^2 \sigma(u)$. But by Lemma 4.3.36 (i), c is unique and thus $c = \sigma(c)$. This holds for all $\sigma \in \mathrm{Gal}(K \mid F)$ and hence $c \in F$.

(ii) Since $m_1 \neq m_2$, $g - c$ is squareful and thus $f - c$ is squareful, by Lemma 4.3.35. By (i), we find $c \in F$. Let $\sigma \in \mathrm{Gal}(K \mid F)$. Then $g_1^{m_1} g_2^{m_2} = g - c = \sigma(g - c) = \sigma(g_1)^{m_1} \sigma(g_2)^{m_2}$. Since $m_1 \neq m_2$, unique factorization implies that $g_i = \sigma(g_i)$ and thus $g_i \in F[x]$ for $i = 1, 2$.

The proof of (iii) is analogous to that of (ii). □

4.4 CLASSIFICATION

> There is no ... Mathematician so expert in his science, as to place entire confidence in any truth immediately upon his discovery of it ... Every time he runs over his proofs, his confidence encreases; but still more by the approbation of his friends; and is raised to its utmost perfection by the universal assent and applauses of the learned world.
>
> — David Hume

We use the results of the previous section to describe in Proposition 4.4.4 the factorization of the components of 2-collisions at degree r^2 satisfying Assumption 4.3.8 over a perfect field F. All non-Frobenius collisions at degree p^2 satisfy this assumption and in Theorem 4.4.9 we provide a complete classification of 2-collisions at that degree over a perfect field. That is, the 2-collisions at degree p^2 are up to original shifting those of Example 4.1.4, Fact 4.2.1, and Theorem 4.2.22. This yields the maximality of these collisions (Corollary 4.4.11) and an efficient algorithm to determine whether a given polynomial $f \in P_{p^2}(F)$ has a 2-collision (Algorithm 4.4.14). In the next section we use this classification to count exactly the decomposable polynomials over a finite F.

Let F be a perfect field and denote by $K = \overline{F}$ an algebraic closure of F.

Definition 4.4.1. Let r be a power of p and $f \in P_{r^2}(F)$ have a 2-collision $\{(g, h), (g^*, h^*)\}$ satisfying Assumption 4.3.8. We call f *multiply original* if there is some $c \in K$ such that $f - c$ has no simple roots in K. Otherwise, we call f *simply original*.

By Lemma 4.3.36 (i), there is at most one $c \in K$ such that $f - c$ is squareful. Since F is perfect, such a c lies in F if it exists, by

Lemma 4.3.38 (i). Furthermore, if f is multiply original, then there is some $c \in F$ such that $f - c$ is squareful. If f is simply original, then either $f - c$ is squarefree for all $c \in K$ or there is a unique $c \in F$ such that $f - c$ is squareful and has a simple root.

Example 4.4.2. Assumption 4.3.8 holds for the 2-collisions $M(a, b, m)$ of Theorem 4.2.22 and the $\#T$-collisions $S(u, s, \varepsilon, m)$ of Fact 4.2.1 with $\#T \geqslant 2$; see Example 4.3.13. Moreover, a polynomial $M(a, b, m)$ has no simple roots and is therefore multiply original. When $\#T \geqslant 2$, then $f = S(u, s, \varepsilon, m)$ is squareful with a simple root if $m > 1$, and $f - c$ is squarefree for all $c \in K$ if $m = 1$.

Proposition 4.4.4 and Theorem 4.4.9 answer the converse question, namely whether every simply original or multiply original polynomial can be obtained as $S(u, s, \varepsilon, m)^{[w]}$ or $M(a, b, m)^{[w]}$, respectively. We need the following graph-theoretic lemma.

Lemma 4.4.3. *Let $G = (V, E)$ be a directed bipartite graph with bipartition $V = A \cup A^*$, where the outdegree of each vertex equals $\ell > 1$ and $\#A = \#A^* = \ell + 1$. Then some vertex in A is connected to all other vertices in A by a path of length 2.*

Proof. Let $A = \{0, \dots, \ell\}$, $A^* = \{\ell + 1, \dots, 2\ell + 1\}$, and M the $(2\ell + 2) \times (2\ell + 2)$ adjacency matrix of G having for each edge from $i \in A \cup A^*$ to $j \in A \cup A^*$ the entry 1 at position (i, j) and entries 0 everywhere else. Since G is bipartite, we have

$$M = \begin{pmatrix} 0 & N \\ N^* & 0 \end{pmatrix},$$

where N and N^* are $(\ell + 1) \times (\ell + 1)$-matrices satisfying the following properties by the assumptions of the lemma.

(i) Each row in N has exactly one entry 0 and all other entries 1.

(ii) Exactly $\ell + 1$ entries of N^* are 0 and all other entries are 1.

The number of paths of length 2 that connect a vertex $i \in A$ to a vertex $j \in A$ is given by the entry (i, j) of

$$M^2 = \begin{pmatrix} N \cdot N^* & 0 \\ 0 & N^* \cdot N \end{pmatrix}.$$

If every column of N^* contains at least two 1's, then $N \cdot N^*$ has only positive entries, because of (i), and every vertex in A is connected to all other vertices in A by a path of length 2. Otherwise, N^* has a column j that contains at most one 1. Because of (ii), every different column of N^* contains at most one 0. Because of $\ell > 1$ and (i), all entries at (j, j') with $j' \neq j$ in $N \cdot N^*$ are positive. Starting from j we can reach all other vertices by a path of length 2. □

Thanks go to Rolf Klein and an anonymous referee for this proof, much simpler than our original one.

Proposition 4.4.4. *Let r be a power of the characteristic $p > 0$ of the perfect field F and let $f \in P_{r^2}(F)$ have a 2-collision $\{(g,h),(g^*,h^*)\}$ satisfying Assumption 4.3.8. Then exactly one of the following holds.*

(s) *The polynomial f is simply original. Let $m = (r-1)/(r-1-\deg g')$. Then there are $w \in F$ and unique monic squarefree polynomials $\hat{f}$, $\hat{g}$, $\hat{h}$, $\hat{g}^*$, and $\hat{h}^*$ in $F[x]$, none of them divisible by x, with $\hat{f}$ of degree $(r^2-1)/m$ and the other four polynomials of degree $r-1-\deg g' = (r-1)/m$ such that*

$$\begin{aligned} f^{[w]} &= x\hat{f}^m, \\ g^{[h(w)]} &= x\hat{g}^m, \\ h^{[w]} &= x\hat{h}^m, \\ (g^*)^{[h^*(w)]} &= x(\hat{g}^*)^m, \\ (h^*)^{[w]} &= x(\hat{h}^*)^m. \end{aligned} \tag{4.4.5}$$

If $\deg f' > 0$, then w is unique. Otherwise, factorizations (4.4.5) with the claimed properties exist for all $w \in F$.

(m) *The polynomial f is multiply original and there are a, b, and m as in Theorem 4.2.22 and $w \in F$ such that*

$$f^{[w]} = M(a,b,m)$$

and the collision $\{(g,h)^{[w]},(g^*,h^*)^{[w]}\}$ is as in Theorem 4.2.22.

Proof. Every polynomial satisfying the assumption of the proposition is either simply original or multiply original by Definition 4.4.1. So, at most one of the two statements holds and it remains to exhibit the claimed parameters in each case. We begin with two general observations.

(i) If $\deg f' = 0$, then $f-c$ is squarefree for all $c \in K$, by Lemma 4.3.4. Thus f is simply original. Moreover, $f^{[w]}$ has derivative $(f^{[w]})' = f' \circ (x+w) = f' \in F^\times$ for all $w \in F$ and is therefore squarefree.

(ii) If $\deg f' > 0$, then there is some $c \in K$ such that $f-c$ has a multiple root by Lemma 4.3.4. Moreover, c is unique by Lemma 4.3.36 (i), and in F by Lemma 4.3.38 (i). Let $\#g^{-1}(c) = \ell+1$ be the number of distinct roots of $g-c$ in K. Then, by Lemma 4.3.36 (ii), g^*-c also has $\ell+1$ roots in K and

$$\ell = r-1-\deg g' \geqslant 1, \tag{4.4.6}$$

by (4.3.37). Let $a_0,\dots,a_\ell$ and $a_0^*,\dots,a_\ell^*$ be the distinct roots of $g-c$ and g^*-c, respectively, and let $e_i = \operatorname{mult}_{a_i}(g-c)$ and $e_i^* = \operatorname{mult}_{a_i^*}(g^*-c)$ be their multiplicities, that is,

$$g-c = \prod_{0\leqslant i\leqslant \ell} (x-a_i)^{e_i}, \quad g^*-c = \prod_{0\leqslant i\leqslant \ell} (x-a_i^*)^{e_i^*}. \tag{4.4.7}$$

By Proposition 4.3.23, for each i and j the set $B_{i,j} = h^{-1}(a_i) \cap h^{*-1}(a_j^*) \subseteq K$ has cardinality $\gcd(e_i, e_j^*)$.

We now deal with the two cases of the theorem separately.

Case (s): Let f be simply original. First, if $\deg f' = 0$, then $\deg g' = 0$, by (4.3.6). Hence $m = (r-1)/(r-1-\deg g') = 1$ and $f^{[w]} = g^{[h(w)]} \circ h^{[w]} = (g^*)^{[h^*(w)]} \circ (h^*)^{[w]}$ is squarefree for all $w \in F$, by (i). Thus the monic polynomials $\hat{f} = f^{[w]}/x$, $\hat{g} = g^{[h(w)]}/x$, $\hat{h} = h^{[w]}/x$, $\hat{g}^* = (g^*)^{[h^*(w)]}/x$, and $\hat{h}^* = (h^*)^{[w]}/x$ are also squarefree and not divisible by x, and (4.4.5) holds for all $w \in F$.

Second, we assume $\deg f' > 0$ for the rest of case (s). By (ii), there is a unique $c \in F$ such that $f - c$ has multiple roots and we assume the notation of (4.4.7) for $g - c$ and $g^* - c$. By the definition of simple originality, $f - c$ has a simple root, say $b_0 \in f^{-1}(c)$. Furthermore, $g - c$ and $g^* - c$ also have simple roots, since

$$1 = \operatorname{mult}_{b_0}(f - c) = \operatorname{lcm}(\operatorname{mult}_{h(b_0)}(g - c), \operatorname{mult}_{h^*(b_0)}(g^* - c))$$

by Proposition 4.3.23. But $g - c$ and $g^* - c$ have at most one simple root by Lemma 4.3.35. We may number the roots so that these unique simple roots are $a_0 = h(b_0)$ and $a_0^* = h^*(b_0)$, both with multiplicity $e_0 = e_0^* = 1$, and $e_i, e_i^* > 1$ for all $i \geqslant 1$.

By Lemma 4.3.28 (ii) and using $e_0^* = 1$, each e_i with $i \geqslant 1$ divides all e_j^* with $j \geqslant 1$. Similarly, each e_j^* with $j \geqslant 1$ divides all e_i with $i \geqslant 1$. Thus all these multiplicities are equal to some integer $m \geqslant 2$, and with $r = \deg g = 1 + \ell m$ from (4.4.7), we have $m = (r-1)/\ell = (r-1)/(r-1-\deg g')$ by (4.4.6). Therefore

$$g - c = (x - a_0)\tilde{g}^m, \quad g^* - c = (x - a_0^*)(\tilde{g}^*)^m$$

with monic squarefree polynomials $\tilde{g} = \prod_{1 \leqslant i \leqslant \ell}(x - a_i)$ and $\tilde{g}^* = \prod_{1 \leqslant i \leqslant \ell}(x - a_i^*) \in K[x]$. We find $a_0, a_0^* \in F$ and $\tilde{g}$, $\tilde{g}^* \in F[x]$ by Lemma 4.3.38 (ii).

Next, we show that $h - a_0$ and $h^* - a_0^*$ have the same root multiplicities as $g^* - c$ and $g - c$, respectively. For $0 \leqslant i \leqslant \ell$, we find from (4.3.27) with the unique $b_i \in B_{0,i}$ and the unique $b_i^* \in B_{i,0}$ as implicitly defined in (ii) that

$$\begin{aligned} \operatorname{mult}_{b_i}(h - a_0) &= \operatorname{lcm}(\operatorname{mult}_{a_0}(g - c), \operatorname{mult}_{a_i^*}(g^* - c)) \\ &= \operatorname{mult}_{a_i^*}(g^* - c), \\ \operatorname{mult}_{b_i^*}(h^* - a_0^*) &= \operatorname{mult}_{a_i}(g - c). \end{aligned}$$

Since $\#B_{0,0} = 1$ by Proposition 4.3.23, we have $b_0 = b_0^*$ and arrive at

$$h - a_0 = (x - b_0)\tilde{h}^m, \quad h^* - a_0^* = (x - b_0)(\tilde{h}^*)^m$$

with monic squarefree polynomials $\tilde{h} = \prod_{1 \leqslant i \leqslant \ell}(x - b_i)$ and $\tilde{h}^* = \prod_{1 \leqslant i \leqslant \ell}(x - b_i^*) \in K[x]$. Again, we find $b_0 \in F$ and $\tilde{h}$, $\tilde{h}^* \in F[x]$, by Lemma 4.3.38 (iii).

Finally, we let $w = b_0$, $\hat{g} = \tilde{g} \circ (x + a_0)$, $\hat{h} = \tilde{h} \circ (x + b_0)$, $\hat{g}^* = \tilde{g}^* \circ (x + a_0^*)$, $\hat{h}^* = \tilde{h}^* \circ (x + b_0)$, and $\hat{f} = \hat{h} \cdot \hat{g}(x\hat{h}^m)$. Then $h(b_0) = a_0$, $f(b_0) = g(h(b_0)) = g(a_0) = c$, and

$$\begin{aligned} g^{[h(w)]} &= (x - c) \circ g \circ (x + a_0) = x\hat{g}^m, \\ h^{[w]} &= (x - a_0) \circ h \circ (x + b_0) = x\hat{h}^m, \\ (g^*)^{[h^*(w)]} &= (x - c) \circ g^* \circ (x + a_0^*) = x(\hat{g}^*)^m, \\ (h^*)^{[w]} &= (x - a_0^*) \circ h^* \circ (x + b_0) = x(\hat{h}^*)^m \end{aligned}$$

with squarefree monic $\hat{g}$, $\hat{g}^*$, $\hat{h}$, and $\hat{h}^*$ of degree $\ell = r - 1 - \deg g'$. Furthermore, $\hat{g}(0) = \tilde{g}(a_0) = \prod_{1 \leqslant i \leqslant \ell}(a_0 - a_i) \neq 0$. This shows that $\hat{g}$ is coprime to x and similar arguments work for $\hat{g}^*$, and for $\hat{h}$ and $\hat{h}^*$ with $b_0 \neq b_i$ for $i \geqslant 1$, since $h(b_0) = a_0 \neq a_i = h(b_i)$ for $i \geqslant 1$. Moreover, $\hat{f} = \hat{h} \cdot \prod_{1 \leqslant i \leqslant \ell}(x\hat{h}^m - a_i + a_0)$ is monic and not divisible by x, and $f^{[w]} = g^{[h(w)]} \circ h^{[w]} = (x\hat{g}^m) \circ (x\hat{h}^m) = x\hat{f}^m$. Since $B_{0,0} = \{b_0\}$ and $\operatorname{lcm}(e_0, e_0^*) = 1$, we find that $f - c$ has a simple root b_0, by Proposition 4.3.23. Furthermore, $f - c$ has $\sum_{i+j \geqslant 1} \#B_{i,j} = 2\ell + \ell^2 m = \ell(r + 1)$ roots with multiplicity m. Thus $\hat{f}$ is squarefree and of degree $\ell(r + 1) = (r^2 - 1)/m$, and the values as claimed in (s) indeed exist.

For the uniqueness in the case $\deg f' > 0$, we consider another factorization $f^{[w_0]} = x\hat{f}_0^m$ satisfying the conditions of case (s). Then $f(x) - f(w) = f^{[w]} \circ (x - w) = (x - w)(\hat{f}(x - w))^m$ and $f(x) - f(w_0) = f^{[w_0]} \circ (x - w_0) = (x - w_0)(\hat{f_0}(x - w_0))^m$. The value for c such that $f - c$ is squareful with a simple root is unique for a simply original polynomial with $\deg f' > 0$, as remarked in (i). Thus $c = f(w) = f(w_0)$ and $(x - w)(\hat{f}(x - w))^m = (x - w_0)(\hat{f_0}(x - w_0))^m$. Since $\deg f' > 0$, we have $\deg g' > 0$ and $m > 1$. Unique factorization yields $w = w_0$ and $\hat{f} = \hat{f_0}$. An analogous argument works for $\hat{g}$, $\hat{g}^*$, $\hat{h}$, and $\hat{h}^*$.

This concludes case (s), and we continue with the case (m).

Case (m): Let f be multiply original. Then $\deg f' > 0$ by (i) from the beginning of the proof. By (ii), there is a unique $c \in F$ such that $f - c$ is squareful, and then $f - c$ has no simple root by Definition 4.4.1 of multiple originality. By Lemma 4.3.35, $g - c$ and $g^* - c$ are also squareful.

Assume that $g - c$ has a simple root. Then $\ell > 0$ and we may number the roots of $g - c$ such that $e_0 = 1$ in the notation (4.4.7). By Lemma 4.3.35, $g - c$ has at most one simple root and thus $e_1 > 1$. By Lemma 4.3.28 (ii), e_1 divides all e_j^* but one and we may number the roots of $g^* - c$ such that $e_1 \mid e_j^*$ for $1 \leqslant j \leqslant \ell$. Interchanging the rôles of g and g^* in Lemma 4.3.28 (ii), we have $e_0^* \mid e_1$ since $e_0 = 1$. Combining these divisibility conditions shows $e_0^* \mid \gcd\{e_j^* : 0 \leqslant j \leqslant \ell\}$ and we find $e_0^* = 1$ from (4.3.29). Hence there exists some $b \in K$ such that $\operatorname{mult}_b(f - c) = \operatorname{lcm}(e_0, e_0^*) = 1$, by Proposition 4.3.23, contradicting Definition 4.4.1 of multiply original by the uniqueness

of c. Therefore $g - c$ has no simple root and $e_i > 1$ for all $i \geqslant 0$. An analogous argument for g^* shows $e_i^* > 1$ for all $i \geqslant 0$.

We now proceed in three steps. First, we determine the factorizations of $g - c$ and $g^* - c$. Second, we derive the factorizations of $h - a_i$ and $h^* - a_i^*$ for the roots $a_i \in g^{-1}(c)$ and $a_i^* \in g^{*-1}(c)$, respectively. Third, we apply an appropriate original shift and prove the claimed form.

To compute ℓ, we translate Proposition 4.3.23 into the language of graphs. We consider the directed bipartite graph on the set $V = A \cup A^*$ of vertices, with disjoint $A = \{i \colon 0 \leqslant i \leqslant \ell\}$ and $A^* = \{i^* \colon 0 \leqslant i \leqslant \ell\}$. The set E of edges consists of all (i, j^*) with $e_i \mid e_j^*$ plus all (i^*, j) with $e_i^* \mid e_j$. Each vertex has outdegree ℓ, by Lemma 4.3.28 (ii), since no root is simple. If $\ell > 1$, then by Lemma 4.4.3 some vertex i in A is connected to all other vertices in A. Then $e_i > 1$ divides all other multiplicities of $g - c$, which contradicts (4.3.29) with g instead of g^*. Hence $\ell = 1$ and therefore

$$\begin{aligned} g - c &= (x - a_0)^{e_0}(x - a_1)^{e_1}, \\ g^* - c &= (x - a_0^*)^{e_0^*}(x - a_1^*)^{e_1^*} \end{aligned}$$

with $1 < e_i, e_i^* < r - 1$, for $i = 0, 1$. We know by Lemma 4.3.28 (i) applied to g and g^*, respectively, that $\gcd(e_0, e_1) = \gcd(e_0^*, e_1^*) = 1$ and since $e_i, e_i^* > 1$ for $i = 0, 1$, each e_i divides exactly one e_j^*, by (ii) of the cited lemma, and similarly each e_j^* divides exactly one e_i. By renumbering if required, we assume $e_0 \mid e_1^*$. If $e_1^* \mid e_1$, then $\gcd(e_0, e_1) = e_0 > 1$, a contradiction to Lemma 4.3.28 (i). Therefore $e_1^* \mid e_0$ and we have $e_0 = e_1^*$. Similar arguments show $e_0^* \mid e_1$ and $e_1 \mid e_0^*$, and hence $e_1 = e_0^*$. We write $m = e_0 = e_1^*$ and $m^* = e_1 = e_0^*$. Then m and m^* are coprime, $m^* = r - m$, since $r = e_0 + e_1$, and $p \nmid m$, by (A_4). Lemma 4.3.38 (ii) yields distinct $a_0, a_1 \in F$ and distinct $a_0^*, a_1^* \in F$ with

$$\begin{aligned} g - c &= (x - a_0)^m (x - a_1)^{m^*}, \\ g^* - c &= (x - a_0^*)^{m^*} (x - a_1^*)^m. \end{aligned}$$

For the sets $B_{i,j}$ defined in (ii), we find $\#B_{0,0} = \#B_{1,1} = 1$, $\#B_{0,1} = m$, and $\#B_{1,0} = m^*$. The multiplicity of each $b_{i,j} \in B_{i,j}$ satisfies

$$\operatorname{mult}_{b_{i,j}}(h - a_i) = \frac{\operatorname{lcm}(e_i, e_j^*)}{e_i} = \begin{cases} m^* & \text{if } i = j = 0, \\ m & \text{if } i = j = 1, \\ 1 & \text{otherwise,} \end{cases}$$

by (4.3.27), and similarly

$$\operatorname{mult}_{b_{i,j}}(h^* - a_j^*) = \begin{cases} m & \text{if } i = j = 0, \\ m^* & \text{if } i = j = 1, \\ 1 & \text{otherwise.} \end{cases}$$

Writing $B_{0,0} = \{b_{0,0}\}$ and $B_{1,1} = \{b_{1,1}\}$, this shows

$$\begin{aligned} h - a_0 &= (x - b_{0,0})^{m^*} H_0, & h - a_1 &= (x - b_{1,1})^m H_0^*, \\ h^* - a_0^* &= (x - b_{0,0})^m H_0^*, & h - a_1^* &= (x - b_{1,1})^{m^*} H_0 \end{aligned}$$

with squarefree monic $H_0 = \prod_{b \in B_{0,1}} (x - b)$ and $H_0^* = \prod_{b \in B_{1,0}} (x - b)$ that do not vanish at $b_{0,0}$ or $b_{1,1}$. Lemma 4.3.38 (iii) implies that $b_{0,0}, b_{1,1} \in F$ and $H_0, H_0^* \in F[x]$.

We use this information to apply the appropriate original shift to our decompositions. Let $w = b_{0,0}$, $a = a_1 - a_0$, $a^* = a_1^* - a_0^*$, and $b = b_{1,1} - b_{0,0}$, with all differences being different from 0, and squarefree monic $H = H_0 \circ (x + w)$ and $H^* = H_0^* \circ (x + w)$. Then $h(w) = a_0$, $h^*(w) = a_0^*$, $g(a_0) = g^*(a_0^*) = c$, and

$$\begin{aligned} g^{[h(w)]} &= x^m (x - a)^{m^*}, \\ h^{[w]} &= x^{m^*} H, \quad h^{[w]} - a = (x - b)^m H^*, \\ g^{*[h^*(w)]} &= x^{m^*} (x - a^*)^m, \\ h^{*[w]} &= x^m H^*, \quad h^{*[w]} - a^* = (x - b)^{m^*} H. \end{aligned} \tag{4.4.8}$$

Equations (4.4.8) yield a system of linear equations

$$\begin{aligned} x^{m^*} H - (x - b)^m H^* &= a, \\ -(x - b)^{m^*} H + x^m H^* &= a^* \end{aligned}$$

over $F(x)$ in H and H^*. We apply Cramer's rule and find

$$\begin{aligned} H &= (a x^m + a^* (x - b)^m)/b^r, \\ H^* &= (a^* x^{m^*} + a (x - b)^{m^*})/b^r, \end{aligned}$$

and $a + a^* = b^r$, since H is monic. Therefore, the polynomials H and H^* are as in (4.2.24) and $f^{[w]} = g^{[h(w)]} \circ h^{[w]} = x^{mm^*} (x - b)^{mm^*} H^m (H^*)^{m^*} = M(a, b, m)$, as in Theorem 4.2.22. □

For 2-collisions at degree p^2, we can refine the classification of Proposition 4.4.4.

Theorem 4.4.9. *Let F be a perfect field of characteristic p and $f \in P_{p^2}(F)$. Then f has a 2-collision $\{(g, h), (g^*, h^*)\}$ if and only if exactly one of the following holds.*

(F) *The polynomial f is a Frobenius collision as in Example 4.1.4.*

(S) *The polynomial f is simply original and there are u, s, ε, and m as in Fact 4.2.1 and $w \in F$ such that*

$$f^{[w]} = S(u, s, \varepsilon, m)$$

and the collision $\{(g, h)^{[w]}, (g^*, h^*)^{[w]}\}$ is contained in the $\#T$-collision described in Fact 4.2.1, with $\#T \geqslant 2$.

(M) *The polynomial* f *is multiply original and there are* a, b, *and* m *as in Theorem 4.2.22 and* $w \in F$ *such that*

$$f^{[w]} = M(a, b, m)$$

and the collision $\{(g, h)^{[w]}, (g^*, h^*)^{[w]}\}$ *is as in Theorem 4.2.22.*

Proof. By Lemma 4.1.6 (i), f is a Frobenius collision if and only if $f' = 0$.

The rest of the proof deals with the case $f' \neq 0$. Assumption 4.3.8 holds by Lemma 4.3.9, the assumptions in Definition 4.4.1 are satisfied, and f is either simply original or multiply original.

For a multiply original f, Proposition 4.4.4 yields the claimed parameters directly, and we now show their existence in the simply original case.

We take $w, m, \hat{g}, \hat{h}$ as in Proposition 4.4.4 (s) and have

$$g^{[h(w)]} = x\hat{g}^m,$$
$$h^{[w]} = x\hat{h}^m.$$

We determine the form of $\hat{g}$ and $\hat{h}$. Let $\ell = \deg \hat{g} = (p-1)/m$. The derivative of $g^{[h(w)]}$ is $\hat{g}^{m-1}(\hat{g} + mx\hat{g}')$, and its degree equals $\deg g' = p - 1 - \ell$, by (4.4.6). Thus $\deg g' = (m-1)\ell + \deg(\hat{g} + mx\hat{g}') = \deg g' + \deg(\hat{g} + mx\hat{g}')$ and $\deg(\hat{g} + mx\hat{g}') = 0$. We write $\hat{g} = \sum_{0 \leqslant i \leqslant \ell} \hat{g}_i x^i$ with $\hat{g}_i \in F$ for all $i \geqslant 0$. Then $\hat{g} + mx\hat{g}' = \sum_{0 \leqslant i \leqslant \ell} (1 + mi)\hat{g}_i x^i$ and we have $\hat{g}_0 \neq 0$ and $(1 + mi)\hat{g}_i = 0$ for all $i \geqslant 1$. Since $1 + mi \neq 0$ in F for $1 \leqslant i < \ell$, it follows that $\hat{g}_i = 0$ for these values of i. Thus we get $\hat{g} = x^\ell - \hat{g}_0$ and $\hat{g}_0 \neq 0$. An analogous argument yields $\hat{h} = x^\ell - \hat{h}_0$ with $\hat{h}_0 \neq 0$. Therefore, we find

$$f^{[w]} = x(x^{\ell(p+1)} - (\hat{h}_0^p + \hat{g}_0)x^\ell + \hat{g}_0\hat{h}_0)^m. \tag{4.4.10}$$

Let

$$(u, s, \varepsilon, t) = \begin{cases} (\hat{g}_0\hat{h}_0, 1, 0, \hat{h}_0) & \text{if } \hat{h}_0^p + \hat{g}_0 = 0, \\ ((\hat{h}_0^p + \hat{g}_0)^{p+1}/(\hat{g}_0\hat{h}_0)^p, & \\ \qquad \hat{g}_0\hat{h}_0/(\hat{h}_0^p + \hat{g}_0), 1, \hat{h}_0/s) & \text{otherwise.} \end{cases}$$

In both cases, u, s, and t are in $F^\times$ and the equations $t^{p+1} - \varepsilon u t + u = 0$, $\hat{h}_0 = st$, $\hat{g}_0 = us^p t^{-1}$, and $f^{[w]} = g^{[h(w)]} \circ h^{[w]} = S(u, s, \varepsilon, m)$ hold. Similarly, we find $g^{*[h^*(w)]} = x(x^\ell - \hat{g}_0^*)^m$ and $h^{*[w]} = x(x^\ell - \hat{h}_0^*)^m$ for some $\hat{g}_0^*, \hat{h}_0^* \in F^\times$, and derive the parameters u^*, s^*, ε^*, and t^* analogously. Since $f^{[w]} = g^{*[h^*(w)]} \circ h^{*[w]}$, it follows from (4.4.10) that $\hat{h}_0^p + \hat{g}_0 = (\hat{h}_0^*)^p + \hat{g}_0^*$ and $\hat{g}_0\hat{h}_0 = \hat{g}_0^*\hat{h}_0^*$. Hence $\varepsilon = \varepsilon^*$, $u = u^*$, and $s = s^*$. Since the decompositions are distinct, we have $t \neq t^*$ and thus $(g, h)^{[w]}$ and $(g^*, h^*)^{[w]}$ are both of the form (4.2.3) with different values for t. □

Corollary 4.4.11. *(i) A polynomial in case* (S) *of Theorem 4.4.9 has a maximal* #T*-collision with* T *as in* (4.2.2).

(ii) A polynomial in case (M) *of Theorem 4.4.9 has a maximal 2-collision.*

Proof. For a polynomial f with collision C and $w \in F$, we write $C^{[w]} = \{(g,h)^{[w]} \colon (g,h) \in C\}$ for the corresponding collision of $f^{[w]}$.

If f is a Frobenius collision as in case (F) of Theorem 4.4.9, then f is maximal by Lemma 4.1.6 (ii). Now let f be a polynomial with a 2-collision $C = \{(g,h),(g^*,h^*)\}$ that does not fall into case (F) of Theorem 4.4.9.

(i) If f falls into case (S) of Theorem 4.4.9, we have by that theorem u, s, ε, and m as in Fact 4.2.1 and $w \in F$ such that $f = S(u,s,\varepsilon,m)^{[-w]}$ and $C \subseteq D(u,s,\varepsilon,m)^{[-w]}$, where $D(u,s,\varepsilon,m)^{[-w]}$ denotes the #T-collision described in Fact 4.2.1 shifted by $-w$.

Take another decomposition $(g_0,h_0) \neq (g,h)$ of f. We apply Theorem 4.4.9 to f with 2-collision $C_0 = \{(g,h),(g_0,h_0)\}$. Due to the mutual exclusivity of the three cases this falls again in case (S), and we obtain u_0, s_0, ε_0, and m_0 as in Fact 4.2.1, and $w_0 \in F$ such that $f = S(u_0,s_0,\varepsilon_0,m_0)^{[-w_0]}$ and $C_0 \subseteq D(u_0,s_0,\varepsilon_0,m_0)^{[-w_0]}$. Thus,

$$f^{[w_0]} = S(u,s,\varepsilon,m)^{[w_0-w]} = S(u_0,s_0,\varepsilon_0,m_0).$$

By Fact 4.2.5 (iv), the only polynomial of the form (4.2.2) in the orbit of $S(u,s,\varepsilon,m)$ under original shifting is the polynomial itself. Therefore,

$$S(u,s,\varepsilon,m) = S(u_0,s_0,\varepsilon_0,m_0). \tag{4.4.12}$$

If $m > 1$, then the stabilizer of $S(u,s,\varepsilon,m)$ under original shifting is $\{0\}$ by Fact 4.2.5 (iii) and we have $w = w_0$. Otherwise, $m = 1$ and $S(u,s,\varepsilon,m)$, $D(u,s,\epsilon,m)$, and $D(u_0,s_0,\epsilon_0,m_0)$ consist only of additive polynomials which are invariant under original shifting. In that case, we can assume $w = w_0$ without loss of generality.

If $\varepsilon = 1$, then Fact 4.2.5 (i) yields $(u,s,\varepsilon,m) = (u_0,s_0,\varepsilon_0,m_0)$ from (4.4.12) and therefore $D(u,s,\varepsilon,m)^{[-w]} = D(u_0,s_0,\varepsilon_0,m_0)^{[-w_0]}$ contains (g_0,h_0). Otherwise, $\varepsilon = 0$ and Fact 4.2.5 (ii) provides $(us^{p+1},\varepsilon,m) = (u_0s_0^{p+1},\varepsilon_0,m_0)$ from (4.4.12). By the definition of $D(u_0,s_0,\varepsilon_0,m_0)^{[-w_0]}$ via Fact 4.2.1, there is some $t_0 \in F$ satisfying $t_0^{p+1} = -u_0$ such that

$$g_0^{[h_0(-w_0)]} = x(x^{p-m_0} - u_0s_0^pt_0^{-1})^{m_0} = x(x^{p-m} - us^pt^{-1})^m,$$
$$h_0^{[-w_0]} = x(x^{p-m_0} - s_0t_0)^{m_0} = x(x^{p-m} - st)^m$$

for $t = t_0s_0/s \in F$. Since t satisfies $t^{p+1} = -u$, this shows $(g_0,h_0) \in D(u,s,\varepsilon,m)^{[-w]}$.

(ii) Let f fall into case (M) of Theorem 4.4.9 and take another decomposition $(g_0,h_0) \neq (g,h)$ of f. We apply that theorem to f with 2-collisions C and $C_0 = \{(g,h),(g_0,h_0)\}$ and obtain a, b, m and a_0, b_0, m_0 as in Theorem 4.2.22 and $w, w_0 \in F$, respectively, such that

$$f = M(a,b,m)^{[-w]} = M(a_0,b_0,m_0)^{[-w_0]},$$

$$C = E(a, b, m)^{[-w]}, \quad \text{and} \quad C_0 = E(a_0, b_0, m_0)^{[-w_0]},$$

where $E(a, b, m)^{[-w]}$ denotes the 2-collision defined in (4.2.23) shifted by $-w$, and $E(a_0, b_0, m_0)^{[-w_0]}$ is analogous. We have

$$M(a, b, m)^{[w_0 - w]} = M(a_0, b_0, m_0). \tag{4.4.13}$$

The only polynomials in the orbit of $M(a, b, m)$ that are of the form (4.2.23) are $M(a, b, m)$ itself and $M(a, b, m)^{[b]}$ according to Proposition 4.2.26 (iv); and by (ii), the stabilizer of $M(a, b, m)$ under original shifting is $\{0\}$. Hence, $w_0 - w = 0$ or $w_0 - w = b$.

If $w_0 = w$, then $M(a_0, b_0, m_0) = M(a, b, m)$ from (4.4.13) and with (iii) of the cited proposition

$$(a_0, b_0, m_0) \in \{(a, b, m), (a^*, b, m^*)\}.$$

If $w_0 = w + b$, then $M(a_0, b_0, m_0) = M(a, b, m)^{[b]} = M(-a^*, -b, m)$ and again with (iii)

$$(a_0, b_0, m_0) \in \{(-a^*, -b, m), (-a, -b, m^*)\}.$$

In either case, we check $E(a_0, b_0, m_0)^{[-w_0]} = E(a, b, m)^{[-w]}$ directly and therefore $(g_0, h_0) \in C$. □

In particular, the polynomials of case (M) have no 3-collision. We combine Theorem 4.4.9 with the algorithms of Section 4.2 for a general test of 2-collisions in Algorithm 4.4.14.

Algorithm 4.4.14: Identify 2-collisions

Input: a polynomial $f \in P_{p^2}(F)$, where $p = \operatorname{char} F$
Output: "(F)", "(S)", or "(M)" as in Theorem 4.4.9, if f has a 2-collision, and "no 2-collision" otherwise

```
if f ∈ F[x^p] \ {x^(p^2)} then return "(F)"
if Algorithm 4.2.18 does not return "failure" on input f, but
  k, u, s, ε, m, w then
    if k ⩾ 2 then return "(S)"
end
if Algorithm 4.2.29 does not return "failure" on input f then
    return "(M)"
end
return "no 2-collision"
```

Theorem 4.4.15. *Algorithm 4.4.14 works correctly as specified. If* $F = \mathbb{F}_q$ *and* $n = p^2 = \deg f$*, it takes* $O(M(n) \log(pq))$ *field operations.*

The correctness follows from Theorem 4.4.9. Its cost is dominated by that of Algorithm 4.2.18, where the $\log n$ factor is subsumed in $\log(pq)$ since $n = p^2$ and $pq \geqslant p^2$. If f is found to have a collision, then that can be returned as well, using Example 4.1.4 for (F).

4.5 COUNTING AT DEGREE p^2

> My work always tried to unite the truth with the beautiful, but when I had to choose one or the other, I usually chose the beautiful.
>
> — Hermann Weyl

The classification of the composition collisions at degree p^2 yields the exact number of decomposable polynomials over a finite field $\mathbb{F}_q$.

Theorem 4.5.1. *Let p be a prime and q a power of p. For $k \geqslant 1$, we write c_k for $\#C_{p^2,k}(\mathbb{F}_q)$ as in (4.1.1), δ for Kronecker's delta function, and τ for the number of positive divisors of $p-1$. Then the following hold.*

$$c_1 = q^{2p-2} - 2q^{p-1} + 2 - \frac{(\tau q - q + 1)(q-1)(qp-q-p)}{p} - (1-\delta_{p,2})\frac{q(q-1)(q-2)(p-3)}{2}, \tag{4.5.2}$$

$$c_2 = q^{p-1} - 1 + \frac{(\tau q - q + 1)(q-1)^2(p-2)}{2(p-1)} + (1-\delta_{p,2})\frac{q(q-1)(q-2)(p-3)}{4}, \tag{4.5.3}$$

$$c_{p+1} = \frac{(\tau q - q + 1)(q-1)(q-p)}{p(p^2-1)}, \tag{4.5.4}$$

$$c_k = 0, \quad \text{if } k \notin \{1, 2, p+1\}. \tag{4.5.5}$$

Proof. For $k \geqslant 2$, we consider $C_k = C_{p^2,k}(\mathbb{F}_q)$. Theorem 4.4.9 provides the partition

$$C_k = C_k^{(F)} \dot\cup C_k^{(S)} \dot\cup C_k^{(M)},$$

where the sets on the right-hand side correspond to the cases (F), (S), and (M), respectively. Lemma 4.1.6 (ii), Proposition 4.2.21, and Corollary 4.2.28 imply that

$$\#C_k^{(F)} = \begin{cases} q^{p-1} - 1 & \text{if } k = 2, \\ 0 & \text{if } k \geqslant 3, \end{cases}$$

$$\#C_k^{(S)} = \begin{cases} \dfrac{(\tau q - q + 1)(q-1)^2(p-2)}{2(p-1)} & \text{if } k = 2, \\ \dfrac{(\tau q - q + 1)(q-1)(q-p)}{p(p^2-1)} & \text{if } k = p+1, \\ 0 & \text{otherwise,} \end{cases}$$

$$\#C_k^{(M)} = \begin{cases} (1-\delta_{p,2})\dfrac{q(q-1)(q-2)(p-3)}{4} & \text{if } k = 2, \\ 0 & \text{if } k \geqslant 3. \end{cases}$$

Summing up yields the exact formulas (4.5.3), (4.5.4), and (4.5.5). Finally, there is a total of q^{2p-2} pairs $(g,h) \in P_p(\mathbb{F}_q) \times P_p(\mathbb{F}_q)$ and therefore (4.5.2) follows from

$$c_1 = q^{2p-2} - \sum_{k \geqslant 2} k \cdot c_k. \qquad \square$$

Equation (4.1.2) now yields the counting result of this chapter, namely the following exact formula for the number of decomposable polynomials of degree p^2 over $\mathbb{F}_q$.

Theorem 4.5.6. *Let $\mathbb{F}_q$ be a finite field of characteristic p, δ Kronecker's delta function, and τ the number of positive divisors of $p-1$. Then*

$$\begin{aligned}\#D_{p^2}(\mathbb{F}_q) = q^{2p-2} - q^{p-1} + 1 - \frac{(\tau q - q + 1)(q-1)(qp-p-2)}{2(p+1)} \\ - (1-\delta_{p,2})\frac{q(q-1)(q-2)(p-3)}{4}.\end{aligned}$$

Proof. By (4.1.2) and Theorem 4.5.1 we find

$$\#D_{p^2}(\mathbb{F}_q) = q^{2p-2} - c_2 - pc_{p+1},$$

from which the claim follows. $\square$

For $p = 2$, this yields

$$\#D_4(\mathbb{F}_q) = q^2 \cdot \frac{2 + q^{-2}}{3},$$

consistent with the result in von zur Gathen (2013). Furthermore, we have

$$\begin{aligned}\#D_9(\mathbb{F}_q) &= q^4\left(1 - \frac{3}{8}(q^{-1} + q^{-2} - q^{-3} - q^{-4})\right) \text{ for } p = 3, \\ \#D_{p^2}(\mathbb{F}_q) &= q^{2p-2}\left(1 - q^{-p+1}\right. \\ &\qquad \left. + O(q^{-2p+5+1/d})\right) \text{ for } q = p^d \text{ and } p \geqslant 5.\end{aligned}$$

We have two independent parameters p and d, and $q = p^d$. For two eventually positive functions $f, g\colon \mathbb{N}^2 \to \mathbb{R}$, here $g \in O(f)$ means that there are constants b and c so that $g(p,d) \leqslant c \cdot f(p,d)$ for all p and d with $p + d \geqslant b$. With the bounds on τ mentioned after the proof of Proposition 4.2.21, we have the following asymptotics.

Corollary 4.5.7. *Let $p \geqslant 5$, $d \geqslant 1$, and $q = p^d$. Then*

$$\begin{aligned}c_1 &= q^{2p-2}(1 - 2q^{-p+1} + O(q^{-2p+5+1/d})), \\ c_2 &= q^{p-1}(1 + O(q^{-p+4+1/d})), \\ c_{p+1} &= (\tau - 1)q^{3-3/d}\left(1 + O(q^{-\max\{2/d, 1-1/d\}})\right) \\ &= O\left(q^{3-3/d+1/(d\log\log p)}\right).\end{aligned}$$

Von zur Gathen (2014a) considers the asymptotics of

$$\nu_{q,n} = \begin{cases} \#D_n/q^{2\ell-2} & \text{if } n = \ell^2, \\ \#D_n/2q^{\ell+n/\ell-2} & \text{otherwise,} \end{cases}$$

where ℓ is the smallest prime divisor of n. It turns out that for any composite n, $\limsup_{q\to\infty} \nu_{q,n} = 1$, and that $\liminf_{q\to\infty} \nu_{q,n} = 1$ for many n. But when ℓ divides n exactly twice, denoted as $\ell^2 \parallel n$, determining the limes inferior was left as an open question. If $n = \ell^2$, we obtain from Theorem 4.5.6

$$\lim_{q\to\infty} \nu_{q,\ell^2} = 1$$

for any prime $\ell > 2$. For $n = 4$, the sequence has no limit, but oscillates between close to $\liminf_{q\to\infty} \nu_{q,4} = 2/3$ and $\limsup_{q\to\infty} \nu_{q,4} = 1$, and these are the only two accumulation points of the sequence $\nu_{q,4}$. If $\ell^2 \parallel n$ and $n \neq \ell^2$, the question of good asymptotics is still open, as it is for $\nu_{q,n}$ when q is fixed and $n \to \infty$.

4.6 CONCLUSION AND FUTURE WORK

I have another question for your answer.

— Joachim von zur Gathen

In the wild case of univariate polynomial decomposition, we have presented some (equal-degree) collisions in the special case where the degree is r^2 for a power r of the characteristic p, and determined their number. We gave a classification of all 2-collisions at degree p^2 and an algorithm which determines whether a given polynomial has a 2-collision, and if so, into which class it falls. We computed the exact number of decomposable polynomials of degree p^2 over finite fields. This gave tight asymptotics on $\nu_{q,n} = \#D_n/q^{2\ell-2}$ for $q \to \infty$, when $n = \ell^2$ is the square of a prime ℓ.

The question of good asymptotics for $\nu_{q,n}$ when q is fixed and $n \to \infty$ is still open. More work is needed to understand the case where the characteristic p is the smallest prime divisor of the degree n, divides n exactly twice, and $n \neq p^2$. Ritt's Second Theorem covers distinct-degree collisions, even in the wild case, under Zannier's mild condition $g'(g^*)' \neq 0$. It would be interesting to see a similar classification for general equal-degree collisions. Finally, the study of rational functions with our method remains open.

ACKNOWLEDGMENTS

However,
not everything that can be counted counts,
and not everything that counts can be counted.
— William Bruce Cameron

Les bons élèves font la gloire du maître.[2]
— Joseph Liouville

I am deeply grateful to my advisor Joachim von zur Gathen. He constantly encouraged me to look for the bigger picture and emphasized clarity of thought and expression. His influence and insight can be felt throughout this thesis. All remaining errors are of course my own.

Furthermore, it is my pleasure to thank Jens Franke and Mark Giesbrecht for serving as referees, and Jaime Gutierrez and Alex Markowetz for joining the doctoral committee. Special thanks go to my co-authors Raoul Blankertz and Tuba Viola for the exciting joint research.

The lion's share of this thesis is based on already published work. Anonymous referees and the audiences at numerous workshops, conferences, and cosec Oberseminar meetings provided plenty of feedback and helpful discussions. Their comments and their patience have been greatly appreciated.

Many colleagues at the University of Bonn and the B-IT have accompanied me along this thesis. I shared an amazing experience with Laila El Aimani, Ismail Khoffi, Martina Kuhnert, Daniel Loebenberger, Michael Nüsken, Alex Pfister, Claudia Oliveira Coelho, Dejan Pejić, Yona Raekow, Alexandra Reitelmann, Anne-Katrin Roesler, and Thomas Thiel. Thank you.

Several teachers have led me by example. I sincerely thank Heinz-Josef Fabry, Lissy Fisch, Franz Graf, Helmut Stumfoll, and Fanny & Hugo Unterpaintner for their guidance and company.

Finally, I am happy and lucky to thank Greg Dachs, Rico Gutschmidt, Silvie Kramer, Mike Lachner, and Mine Lφ Reimnitz for being my friends. And last, but not least, I am grateful to my mother and my brother for being my family.

Konstantin Ziegler
Bonn, June 2014

[2] Good students are the teacher's glory.

Part III

APPENDIX

SOURCE CODE

> Rule 8: The development of fast algorithms is slow!
> — Arnold Schönhage

> Beware of bugs in the above code; I have only proved it correct, not tried it.
> — Donald E. Knuth

> With this situation [closed source] two of the most basic rules of conduct in mathematics are violated: In mathematics information is passed on free of charge and everything is laid open for checking.
> — Joachim Neubüser

We have implemented all our counting formulas to adhere to Don Knuth's warning. We also gladly follow Joachim Neubüser's appeal and make the implementations public. The `Sage` code is available at

- `https://github.com/zieglerk/multivariate_polynomials` and
- `https://github.com/zieglerk/polynomial_decomposition`

for Part i and ii, respectively.

SOURCES OF QUOTATIONS

I hate quotation. Tell me what you know.
— Ralph Waldo Emerson

I don't necessarily agree with everything that I say.
— Marshall McLuhan

page 1: Bundesministerium für Bildung und Forschung, *Jahr der Mathematik 2008*, available at `http://www.jahr-der-mathematik.de/` (last accessed 2014/05/31).
page 1: Doron Zeilberger, *Title of a lecture at the Conference in Honor of Doron Zeilberger's 60th Birthday*, delivered on August 14, 2010, available at `www.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/hard.html` (last accessed 2014/05/30).
page 1: Tom Stoppard, *Jumpers*, Act I, 1972.
page 1: Elizabeth Barrett Browning, *Sonnets from the Portuguese*, Number 43, 1850.
page 1: Rudyard Kipling, *Just So Stories*, 1902.
page 1: Leopold Kronecker, Vortrag bei der Berliner Naturforscher-Versammlung, 1886.
page 2: Agatha Christie, *Murder on the Orient Express*, 1934.
page 5: Isaac Newton, attributed
page 7: Robert Boyle, *Some Considerations touching the Usefulness of Experimental Natural Philosophy*, vol. 2, *The Usefulness of Mathematicks to Natural Philosophy*, Oxford, 1671.
page 9: Dick Lipton, *The More Variables, the Better?*, available at `http://rjlipton.wordpress.com/2014/04/16/the-more-variables-the-better/` (last accessed 2014/06/02).
page 11: Leonard Carlitz, *The arithmetic of polynomials in a Galois field*, American Journal of Mathematics 54, pp. 39–50, 1932, p. 39.
page 13: Epictetus, *Discourses*, Book I, Chapter 18.
page 13: Arthur Conan Doyle, *The crooked man*, published in *The Memoirs of Sherlock Holmes*, 1893. page 22: Augusta Ada Lovelace, *Sketch of the Analytical Engine Invented by Charles Babbage*, Esq., by L. F. Menabrea (translated and with notes by "A. A. L."). *Taylor's Scientific Memoirs* 3 (1843), Article XXIX, 666–731.
page 27: Dick Guindon, *cartoon*, San Francisco Chronicle, January 1989.
page 27: Leslie Lamport, *Specifying Systems*, Boston, 2002, p. 2.
page 38: Donald E. Knuth, *Turing Award Lecture*, Communications of the ACM 17 (12), pp. 667–673, December 1974, p. 671.
page 51: Alfred North Whitehead, *An Introduction to Mathematics*, 1911, Chapter 5.
page 53: Donald E. Knuth, *Turing Award Lecture*, Communications of the ACM 17 (12), pp. 667–673, December 1974, pp. 668–669.

page 53: Eric Temple Bell, *Men of Mathematics I*, ch. 2: Modern minds in ancient bodies, Penguin Books, 1937, p. 33.
page 55: Serge Lang, *Math Talks for Undergraduates*, Springer, 1999.
page 57: Al Cuoco, E. Paul Goldenberg, June Mark, *Habits of Mind: An Organizing Principle Form Mathematics Curriculum*, Journal of Mathematical Behavior 15, pp. 375–402, 1996, available at `http://jwilson.coe.uga.edu/EMAT7050/Cuoco.HabitsOfMind.pdf`.
page 58: Herman Melville, *Moby Dick*, 1851, Chapter 32.
page 62: Paul Halmos, *Four panel talks on publishing*, American Mathematical Monthly 82, pp. 14–17, 1975.
page 72: Andrew Granville, *Don't be seduced by the zeros!*, available at `http://www.dms.umontreal.ca/~andrew/PDF/CMSNotes.pdf`, p. 2.
page 77: Galileo Galilei, attributed, in Timothy Rasinski and Lorraine Griffith, *Building Fluency Through Practice and Performance*, 2008, p. 64.
page 84: David Hilbert, *Mathematical Problems*, Bulletin American Mathematical Society, Volume 8, Number 10, 1902, available at `http://www.ams.org/journals/bull/1902-08-10/S0002-9904-1902-00923-3/`, p. 438.
page 87: Gertrude Stein, *Composition as Explanation*, 1926.
page 88: Oystein Ore, *On the foundations of abstract algebra, I.* Annals of Mathematics 36, pp. 406–37, 1935.
page 90: Volker Strassen, *Asymptotic spectrum and matrix multiplication*, invited talk at ISSAC'12, delivered on July 24, 2012.
page 103: Ernst Mach, *Popular Scientific Lectures*, Chicago, 1894, available at `http://www.gutenberg.org/files/39508/39508-h/39508-h.htm`, p. 205.
page 117: David Hume, *A Treatise of Human Nature*, 1739, available at `http://www.gutenberg.org/files/4705/4705-h/4705-h.htm`.
page 127: Hermann Weyl, *Gesammelte Abhandlungen*, 4 Volumes, edited by K. Chandrasekharan, 1968.
page 129: Joachim von zur Gathen, question to the author in the cosec Oberseminar on May 8, 2014.
page 131: Joseph Liouville, Œuvres mathématiques d'Évariste Galois, *Journal de mathématiques pures et appliquées* 9, pp. 381–444, 1846, p. 381.
page 131: William Bruce Cameron, *Informal Sociology: A Casual Introduction to Sociological Thinking*, 1963, p. 13.
page 135: J. Neubüser, *An Invitation to Computational Group Theory*, Groups'93 Galway/St. Andrews, Vol. 2, 457–475, London Math. Soc. Lecture Note Ser., 212, Cambridge Univ. Press, Cambridge, 1995. Preprint available at `http://www.gap-system.org/Doc/Talks/cgt.ps`, p. 16.
page 135: Arnold Schönhage, Andreas F. W. Grotefeld, Ekkehard Vetter, *Fast Algorithms: A Multitape Turing Machine Implementation*, BI-Wissenschaftsverlag, Mannheim, 1994, p. 284.
page 135: Donald E. Knuth, *Notes on the van Emde Boas construction of priority deques: An instructive use of recursion*, 1977, p. 5.
page 137: Marshall McLuhan, attributed.
page 137: Ralph Waldo Emerson, *Journals*, May, 1849.
page 141: Woodrow Wilson, *Speech to the National Press Club*, delivered on March 20, 1914.

LIST OF FIGURES

LIST OF TABLES

BIBLIOGRAPHY

I not only use all the brains I have,
but all I can borrow.
— Woodrow Wilson

Max Alekseyev (2006). A115457–A115472. In *The On-Line Encyclopedia of Integer Sequences*. OEIS Foundation Inc. URL `http://oeis.org`. Last download 4 December 2012. (Cited on page 21.)

T. M. Apostol (1976). *Introduction to Analytic Number Theory*. Springer-Verlag, New York. (Cited on page 84.)

E. Artin (1924). Quadratische Körper im Gebiete der höheren Kongruenzen. II. (Analytischer Teil.). *Mathematische Zeitschrift* **19**(1), 207–246. URL `http://dx.doi.org/10.1007/BF01181075`. (Cited on page 9.)

Roberto M. Avanzi & Umberto M. Zannier (2003). The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$. *Compositio Math.* **139**(3), 263–295. URL `http://dx.doi.org/10.1023/B:COMP.0000018136.23898.65`. (Cited on page 97.)

Eric Bach & Jeffrey Shallit (1997). *Algorithmic Number Theory, Vol.1: Efficient Algorithms*. MIT Press, Cambridge MA, second printing edition. ISBN 0-262-02405-5. (Cited on page 69.)

David R. Barton & Richard Zippel (1985). Polynomial Decomposition Algorithms. *Journal of Symbolic Computation* **1**, 159–168. (Cited on page 55.)

Raoul Blankertz (2011). *Decomposition of Polynomials*. Diplomarbeit, Universität Bonn. Modified version available at `http://arxiv.org/abs/1107.0687`. (Cited on pages 88 and 104.)

Raoul Blankertz (2014). A polynomial time algorithm for computing all minimal decompositions of a polynomial. *ACM Communications in Computer Algebra* **48**(1), 13–23. Issue 187. (Cited on page 55.)

Raoul Blankertz, Joachim von zur Gathen & Konstantin Ziegler (2013). Compositions and collisions at degree p^2. *Journal of Symbolic Computation* **59**, 113–145. ISSN 0747-7171. URL `http://dx.doi.org/10.1016/j.jsc.2013.06.001`. Also available at `http://arxiv.org/abs/1202.5810`. Extended abstract in *Proceedings of the 2012 International Symposium on Symbolic and Algebraic*

Computation ISSAC 2012, Grenoble, France (2012), 91–98. (Cited on page 87.)

Antonia W. Bluher (2004). On $x^{q+1} + ax + b$. *Finite Fields and Their Applications* **10**(3), 285–305. URL http://dx.doi.org/10.1016/j.ffa.2003.08.004. (Cited on page 91.)

Arnaud Bodin (2008). Number of irreducible polynomials in several variables over finite fields. *American Mathematical Monthly* **115**(7), 653–660. ISSN 0002-9890. (Cited on pages 9 and 21.)

Arnaud Bodin (2010). Generating series for irreducible polynomials over finite fields. *Finite Fields and Their Applications* **16**(2), 116–125. URL http://dx.doi.org/10.1016/j.ffa.2009.11.002. (Cited on pages 10 and 21.)

Arnaud Bodin, Pierre Dèbes & Salah Najib (2009). Indecomposable polynomials and their spectrum. *Acta Arithmetica* **139(1)**, 79–100. (Cited on page 10.)

Jan Büthe (2014). A Practical Analytic Method For Calculating $\pi(x)$ II. *Preprint*, 21 pages. (Cited on page 2.)

John J. Cade (1985). A New Public-key Cipher Which Allows Signatures. In *Proceedings of the 2nd SIAM Conference on Applied Linear Algebra*. SIAM, Raleigh NC. (Cited on page 55.)

M. Car (1987). Théorèmes de densité dans $\mathbb{F}_q[X]$. *Acta Arithmetica* **48**, 145–165. (Cited on page 9.)

Leonard Carlitz (1932). The arithmetic of polynomials in a Galois field. *American Journal of Mathematics* **54**, 39–50. (Cited on pages 27 and 30.)

Leonard Carlitz (1963). The distribution of irreducible polynomials in several indeterminates. *Illinois Journal of Mathematics* **7**, 371–375. (Cited on pages 3 and 9.)

Leonard Carlitz (1965). The distribution of irreducible polynomials in several indeterminates II. *Canadian Journal of Mathematics* **17**, 261–266. (Cited on page 9.)

Eda Cesaratto, Joachim von zur Gathen & Guillermo Matera (2013). The number of reducible space curves over a finite field. *Journal of Number Theory* **133**, 1409–1434. URL http://dx.doi.org/10.1016/j.jnt.2012.08.027. (Cited on page 10.)

Stephen Cohen (1968). The distribution of irreducible polynomials in several indeterminates over a finite field. *Proceedings of the Edinburgh Mathematical Society* **16**, 1–17. (Cited on pages 9 and 17.)

Stephen Cohen (1969). Some arithmetical functions in finite fields. *Glasgow Mathematical Society* **11**, 21–36. (Cited on page 9.)

Stephen D. Cohen (1985). Reducibility of sub-linear polynomials over a finite field. *Bulletin of the Korean Mathematical Society* **22**, 53–56. (Cited on page 90.)

Stephen D. Cohen (1990a). Exceptional polynomials and the reducibility of substitution polynomials. *Enseign. Math. (2)* **36**(1-2), 53–65. ISSN 0013-8584. (Cited on page 90.)

Stephen D. Cohen (1990b). The Factorable Core of Polynomials Over Finite Fields. *Journal of the Australian Mathematical Society, Series A* **49**(02), 309–318. URL http://dx.doi.org/10.1017/S1446788700030585. (Cited on pages 90 and 108.)

Stephen D. Cohen & Rex W. Matthews (1994). A class of exceptional polynomials. *Transactions of the American Mathematical Society* **345**(2), 897–909. ISSN 0002-9947. URL http://www.jstor.org/stable/2155005. (Cited on page 90.)

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest & Clifford Stein (2009). *Introduction to Algorithms*. MIT Press, Cambridge MA, London UK, 3rd edition. ISBN 978-0-262-03384-8 (hardcover), 978-0-262-53305-8 (paperback), 1312 pages . (Cited on pages 74 and 79.)

Robert S. Coulter, George Havas & Marie Henderson (2004). On decomposition of sub-linearised polynomials. *Journal of the Australian Mathematical Society* **76**(3), 317–328. ISSN 1446-7887. URL http://dx.doi.org/10.1017/S1446788700009885. (Cited on page 90.)

L. E. Dickson (1897). The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. Part I & II. *Annals of Mathematics* **11**, 65–120, 161–183. URL http://www.jstor.org/stable/1967217,http://www.jstor.org/stable/1967224. (Cited on page 90.)

F. Dorey & G. Whaples (1974). Prime and Composite Polynomials. *Journal of Algebra* **28**, 88–101. URL http://dx.doi.org/10.1016/0021-8693(74)90023-4. (Cited on pages 55, 90, 104, and 110.)

H. T. Engstrom (1941). Polynomial Substitutions. *American Journal of Mathematics* **63**, 249–255. URL http://www.jstor.org/stable/2371520. (Cited on page 55.)

Howard Eves (1990). *Introduction to the History of Mathematics*. Saunders College Publishing, Philadelphia PA, 6th edition. (Cited on page 1.)

P. Flajolet, X. Gourdon & D. Panario (2001). The Complete Analysis of a Polynomial Factorization Algorithm over Finite Fields. *Journal of Algorithms* **40**(1), 37–81. Extended Abstract in *Proceedings of the 23rd International Colloquium on Automata, Languages and Programming ICALP 1996*, Paderborn, Germany, ed. F. Meyer auf der Heide and B. Monien, Lecture Notes in Computer Science **1099**, Springer-Verlag, 1996, 232–243. (Cited on page 27.)

Philippe Flajolet & Robert Sedgewick (2009). *Analytic Combinatorics*. Cambridge University Press. ISBN 0521898064, 824 pages. (Cited on pages 10, 11, 12, 16, and 27.)

Jens Franke, Thorsten Kleinjung, Jan Büthe & Alexander Jost (2014). A Practical Analytic Method For Calculating $\pi(x)$. *Submitted*, 20 pages. (Cited on page 2.)

Michael D. Fried & R. E. MacRae (1969). On the invariance of chains of fields. *Illinois Journal of Mathematics* **13**, 165–171. (Cited on pages 55 and 109.)

C. Fuchs & A. Pethő (2011). Composite rational functions having a bounded number of zeros and poles. *Proceedings of the American Mathematical Society* **139**(1), 31–38. ISSN 1088-6826(online) ISSN 0002-9939(print). URL http://www.ams.org/journals/proc/2011-139-01/S0002-9939-2010-10684-6/. (Cited on page 56.)

Clemens Fuchs & Umberto Zannier (2012). Composite Rational Functions Expressible with new Terms. *Journal of the European Mathematical Society* **14**(1), 175–208. URL http://dx.doi.org/10.4171/JEMS/299. (Cited on page 56.)

Shuhong Gao & Alan G. B. Lauder (2002). Hensel Lifting and Bivariate Polynomial Factorisation over Finite Fields. *Mathematics of Computation* **71**(240), 1663–1676. URL http://dx.doi.org/10.1090/S0025-5718-01-01393-X. (Cited on page 9.)

Joachim von zur Gathen (1990a). Functional Decomposition of Polynomials: the Tame Case. *Journal of Symbolic Computation* **9**, 281–299. URL http://dx.doi.org/10.1016/S0747-7171(08)80014-4. Extended abstract in *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science, Los Angeles CA* (1987). (Cited on pages 55 and 89.)

Joachim von zur Gathen (1990b). Functional Decomposition of Polynomials: the Wild Case. *Journal of Symbolic Computation* **10**, 437–452. URL http://dx.doi.org/10.1016/S0747-7171(08)80054-5. (Cited on page 55.)

Joachim von zur Gathen (2002). Factorization and Decomposition of Polynomials. In *The Concise Handbook of Algebra*, edited by

Alexander V. Mikhalev & Günter F. Pilz, 159–161. Kluwer Academic Publishers. ISBN 0-7923-7072-4. (Cited on page 55.)

Joachim von zur Gathen (2008). Counting reducible and singular bivariate polynomials. *Finite Fields and Their Applications* **14**(4), 944–978. URL http://dx.doi.org/10.1016/j.ffa.2008.05.005. Extended abstract in *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation ISSAC '07, Waterloo, Ontario, Canada* (2007), 369-376. (Cited on pages 9, 10, 14, 26, 29, 37, 40, 50, and 51.)

Joachim von zur Gathen (2011). Counting decomposable multivariate polynomials. *Applicable Algebra in Engineering, Communication and Computing* **22**(3), 165–185. URL http://dx.doi.org/10.1007/s00200-011-0141-9. Abstract in *Abstracts of the Ninth International Conference on Finite Fields and their Applications*, pages 21–22, Dublin, July 2009, Claude Shannon Institute, http://www.shannoninstitute.ie/fq9/AllFq9Abstracts.pdf. (Cited on page 10.)

Joachim von zur Gathen (2013). Lower bounds for decomposable univariate wild polynomials. *Journal of Symbolic Computation* **50**, 409–430. URL http://dx.doi.org/10.1016/j.jsc.2011.01.008. (Cited on pages 106, 109, and 128.)

Joachim von zur Gathen (2014a). Counting decomposable univariate polynomials. *Combinatorics, Probability and Computing, Special Issue 01* **24**, 294–328. URL http://dx.doi.org/10.1017/S0963548314000388. Extended abstract in *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation ISSAC '09, Seoul, Korea* (2009). Preprint (2008) available at http://arxiv.org/abs/0901.0054. (Cited on pages 4, 56, 83, 85, 88, 97, and 129.)

Joachim von zur Gathen (2014b). Normal form for Ritt's Second Theorem. *Finite Fields and Their Applications* **27**, 41–71. ISSN 1071-5797. URL http://dx.doi.org/10.1016/j.ffa.2013.12.004. Also available at http://arxiv.org/abs/1308.1135. (Cited on pages 4, 56, 57, 60, and 61.)

Joachim von zur Gathen & Jürgen Gerhard (2013). *Modern Computer Algebra*. Cambridge University Press, Cambridge, UK, Third edition. ISBN 9781107039032. URL http://cosec.bit.uni-bonn.de/science/mca/. Other editions: 1999, 2003, Chinese edition, Japanese translation. (Cited on page 103.)

Joachim von zur Gathen, Mark Giesbrecht & Konstantin Ziegler (2010). Composition collisions and projective polynomials. Statement of results. In *Proceedings of the 2010 International*

Symposium on Symbolic and Algebraic Computation ISSAC '10, Munich, Germany, edited by Stephen Watt, 123–130. ACM Press. URL http://dx.doi.org/10.1145/1837934.1837962. Preprint available at http://arxiv.org/abs/1005.1087. (Cited on pages 88, 91, 95, 96, and 105.)

Joachim von zur Gathen, Dexter Kozen & Susan Landau (1987). Functional Decomposition of Polynomials. In *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science, Los Angeles CA*, 127–131. IEEE Computer Society Press, Washington DC. URL http://dx.doi.org/10.1109/SFCS.1987.29. (Cited on page 55.)

Joachim von zur Gathen, Alfredo Viola & Konstantin Ziegler (2013). Counting reducible, powerful, and relatively irreducible multivariate polynomials over finite fields. *SIAM Journal on Discrete Mathematics* **27**(2), 855–891. URL http://dx.doi.org/10.1137/110854680. Also available at http://arxiv.org/abs/0912.3312. Extended abstract in *Proceedings of LATIN 2010, Oaxaca, Mexico*, volume 6034 of *Lecture Notes in Computer Science*, 243–254 (2010). (Cited on page 9.)

Joachim von zur Gathen & Konstantin Ziegler (2015). Survey on counting special types of polynomials. In *Computer Algebra and Polynomials*, edited by Jaime Gutierrez, Josef Schicho & Martin Weimann, volume 8942 of *Lecture Notes in Computer Science*, 1–26. Springer-Verlag, Berlin, Heidelberg. URL http://dx.doi.org/10.1007/978-3-319-15081-9_3. Also available at http://arxiv.org/abs/1407.2970. (Cited on page 6.)

Mark William Giesbrecht (1988). *Some Results on the Functional Decomposition of Polynomials*. Master's thesis, Department of Computer Science, University of Toronto. Technical Report 209/88. Available as http://arxiv.org/abs/1004.5433. (Cited on pages 4, 56, and 90.)

Sudesh K. Gogia & Indar S. Luthar (1981). Norms from certain extensions of $F_q(T)$. *Acta Arithmetica* **38**(4), 325–340. ISSN 0065-1036. (Cited on page 9.)

David Goss (1996). *Basic Structures of Function Field Arithmetic*. Springer-Verlag. ISBN 3-540-61087-1. (Cited on page 90.)

Johannes Grabmeier, Erich Kaltofen & Volker Weispfenning (editors) (2003). *Computer Algebra Handbook – Foundations, Applications, Systems*. Springer-Verlag, Berlin, Heidelberg, New York. ISBN 3-540-65466-6. URL http://www.springer.com/978-3-540-65466-7. (Cited on page 147.)

R. L. Graham, D. E. Knuth & O. Patashnik (1989). *Concrete Mathematics*. Addison-Wesley, Reading MA. (Cited on page 30.)

Jaime Gutierrez & Dexter Kozen (2003). Polynomial Decomposition. In Grabmeier, Kaltofen & Weispfenning (2003), section 2.2.4 (pages 26–28). URL http://www.springer.com/978-3-540-65466-7. (Cited on page 55.)

Jaime Gutierrez & David Sevilla (2006a). Building counterexamples to generalizations for rational functions of Ritt's decomposition theorem. *Journal of Algebra* **303**(2), 655–667. URL http://dx.doi.org/10.1016/j.jalgebra.2006.06.015. Also available at http://arxiv.org/abs/0804.1687. (Cited on page 84.)

Jaime Gutierrez & David Sevilla (2006b). On Ritt's decomposition theorem in the case of finite fields. *Finite Fields and Their Applications* **12**(3), 403–412. URL http://dx.doi.org/10.1016/j.ffa.2005.08.004. Also available at http://arxiv.org/abs/0803.3976. (Cited on page 55.)

R. W. Hamming (1987). *Numerical Methods for Scientists and Engineers*. Dover Publications, Inc., 2nd edition. (Cited on page 2.)

G. H. Hardy & E. M. Wright (1985). *An introduction to the theory of numbers*. Clarendon Press, Oxford, 5th edition. First edition 1938. (Cited on pages 84 and 97.)

David. R. Hayes (1965). The Distribution of Irreducibles in GF[q, x]. *Transactions of the American Mathematical Society* **117**, 101–127. URL http://dx.doi.org/10.2307/1994199. (Cited on page 9.)

D. R. Heath-Brown (1992). Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression. *Proceedings of the London Mathematical Society* **64**, 265–338. (Cited on page 97.)

Marie Henderson & Rex Matthews (1999). Composition behaviour of sub-linearised polynomials over a finite field. In *Finite Fields: Theory, Applications, and Algorithms (Waterloo, ON, 1997)*, volume 225 of *Contemp. Math.*, 67–75. Amer. Math. Soc., Providence, RI. (Cited on pages 90 and 107.)

Xiang-dong Hou & Gary L. Mullen (2009). Number of Irreducible Polynomials and Pairs of Relatively Prime Polynomials in Several Variables over Finite Fields. *Finite Fields and Their Applications* **15**(3), 304–331. URL http://dx.doi.org/10.1016/j.ffa.2008.12.004. (Cited on pages 10, 21, and 51.)

M. N. Huxley (2003). Exponential sums and lattice points III. *Proceedings of the London Mathematical Society* **87**(3), 591–609. (Cited on page 84.)

Nathan Jacobson (1964). *Lectures in abstract algebra: Volume III – Theory of fields and Galois theory*. Van Nostrand. ISBN 9780387901688. (Cited on pages 111 and 112.)

Arnold Knopfmacher & Michael Mays (2006). Ordered and Unordered Factorizations of Integers. *The Mathematica Journal* **10**(1), 72–89. URL http://www.mathematica-journal.com/issue/v10i1/contents/Factorizations/Factorizations.pdf. (Cited on page 62.)

Donald E. Knuth (1973). *The Art of Computer Programming, vol.1: Fundamental Algorithms*. Addison-Wesley, Reading MA, 2nd edition. (Cited on page 79.)

Donald E. Knuth (1992). Two notes on notation. *The American Mathematical Monthly* **99**(5), 403–422. URL http://arxiv.org/abs/math/9205211. (Cited on page 11.)

Dexter Kozen & Susan Landau (1989). Polynomial Decomposition Algorithms. *Journal of Symbolic Computation* **7**, 445–456. URL http://dx.doi.org/10.1016/S0747-7171(89)80027-6. An earlier version was published as Technical Report 86-773, Cornell University, Department of Computer Science, Ithaca, New York, 1986. (Cited on page 55.)

Dexter Kozen, Susan Landau & Richard Zippel (1996). Decomposition of Algebraic Functions. *Journal of Symbolic Computation* **22**, 235–246. (Cited on page 55.)

S. Landau & G. L. Miller (1985). Solvability by Radicals is in Polynomial Time. *Journal of Computer and System Sciences* **30**, 179–208. (Cited on page 55.)

Serge Lang (2002). *Algebra*. Springer-Verlag. ISBN 9780387953854. (Cited on pages 109 and 111.)

Howard Levi (1942). Composite polynomials with coefficients in an arbitrary field of characteristic zero. *American Journal of Mathematics* **64**, 389–400. (Cited on page 55.)

Rudolf Lidl & Harald Niederreiter (1997). *Finite Fields*. Number 20 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, UK, 2nd edition. First published by Addison-Wesley, Reading MA, 1983. (Cited on page 16.)

Richard J. Lipton (2014). Counting Edge Colorings Is Hard. Webpage. URL http://rjlipton.wordpress.com/2014/06/23/counting-edge-colorings-is-hard/. Last download 28 June 2014. (Cited on page 2.)

FLORIAN LUCA & IGOR E. SHPARLINSKI (2008). On the values of the divisor function. *Monatshefte für Mathematik* **154**, 59–69. URL http://dx.doi.org/10.1007/s00605-007-0511-3. (Cited on page 97.)

ALICE MEDVEDEV & THOMAS SCANLON (2014). Invariant varieties for polynomial dynamical systems. *Annals of Mathematics* **179**(1), 81–177. URL http://dx.doi.org/10.4007/annals.2014.179.1.2. Also available at http://arxiv.org/abs/0901.2352v3. (Cited on page 57.)

GARY L. MULLEN & DANIEL PANARIO (2013). *Handbook of Finite Fields*. Discrete Mathematics and Its Applications. CRC Press, Boca Raton, FL, USA. ISBN 978-1-4398-7378-6 (Hardback). URL http://www.crcpress.com/product/isbn/9781439873786. (Cited on page 9.)

JÜRGEN NEUKIRCH (1999). *Algebraic Number Theory*. Springer-Verlag. ISBN 3-540-65399-6. (Cited on page 110.)

O. ORE (1933). On a Special Class of Polynomials. *Transactions of the American Mathematical Society* **35**, 559–584. (Cited on pages 90 and 108.)

J. F. RITT (1922). Prime and Composite Polynomials. *Transactions of the American Mathematical Society* **23**, 51–66. URL http://www.jstor.org/stable/1988911. (Cited on page 60.)

ANDRZEJ SCHINZEL (1982). *Selected Topics on Polynomials*. Ann Arbor; The University of Michigan Press. ISBN 0-472-08026-1. (Cited on page 55.)

ANDRZEJ SCHINZEL (2000). *Polynomials with special regard to reducibility*. Cambridge University Press, Cambridge, UK. ISBN 0521662257. (Cited on pages 55 and 56.)

W. A. STEIN *et al.* (2014). *Sage Mathematics Software (Version 6.1.1)*. The Sage Development Team. URL http://www.sagemath.org. (Cited on pages 85, 135, and 153.)

HENNING STICHTENOTH (2009). *Algebraic Function Fields and Codes*. Springer-Verlag. ISBN 978-3-540-76877-7. (Cited on pages 110 and 111.)

ROBERT ENDRE TARJAN (1976). Edge-Disjoint Spanning Trees and Depth-First Search. *Acta Informatica* **6**, 171–185. URL http://dx.doi.org/10.1007/BF00268499. (Cited on page 79.)

PIERRE TORTRAT (1988). Sur la composition des polynômes. *Colloquium Mathematicum* **55**(2), 329–353. (Cited on page 61.)

GERHARD TURNWALD (1995). On Schur's Conjecture. *Journal of the Australian Mathematical Society, Series A* **58**, 312–357. URL http://

anziamj.austms.org.au/JAMSA/V58/Part3/Turnwald.html. (Cited on page 55.)

Daqing Wan (1992). Zeta Functions of Algebraic Cycles over Finite Fields. *Manuscripta Mathematica* **74**, 413–444. (Cited on page 9.)

David Wells (1990). Are These the Most Beautiful? *The Mathematical Intelligencer* **12**(3), 37–41. URL http://dx.doi.org/10.1007/BF03024015. (Cited on page 2.)

S. Wigert (1907). Sur l'ordre de grandeur du nombre des diviseurs d'un entier. *Arkiv för matematik, astronomi och fysik* **3**(18), 1–9. (Cited on page 84.)

Eugene P. Wigner (1960). The unreasonable effectiveness of mathematics in the Natural Sciences. *Communications in Pure and Applied Mathematics* **13**(1), 1–14. URL http://dx.doi.org/10.1002/cpa.3160130102. (Cited on page 2.)

Kenneth S. Williams (1969). Polynomials with irreducible factors of specified degree. *Canadian Mathematical Bulletin* **12**, 221–223. ISSN 0008-4395. (Cited on page 9.)

Triantafyllos Xylouris (2011). Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression. Dissertation. Rheinische Friedrich-Wilhelms-Universität Bonn. (Cited on page 97.)

U. Zannier (1993). Ritt's Second Theorem in arbitrary characteristic. *Journal für die reine und angewandte Mathematik* **445**, 175–203. URL http://eudml.org/doc/153580. (Cited on pages 55, 56, and 104.)

Umberto Zannier (2007). On the number of terms of a composite polynomial. *Acta Arithmetica* **127**, 157–167. URL http://dx.doi.org/10.4064/aa127-2-5. (Cited on page 56.)

Umberto Zannier (2008). On composite lacunary polynomials and the proof of a conjecture of Schinzel. *Inventiones mathematicae* **174**, 127–138. ISSN 0020-9910 (Print) 1432-1297 (Online). URL http://dx.doi.org/10.1007/s00222-008-0136-8. Also available at http://arxiv.org/abs/0705.0911v1. (Cited on page 56.)

Umberto Zannier (2009). Addendum to the paper: On the number of terms of a composite polynomial. *Acta Arithmetica* **140**, 93–99. URL http://dx.doi.org/10.4064/aa140-1-6. (Cited on page 56.)

Konstantin Ziegler (2014). Tame decompositions and collisions. *Submitted,* 35 pages. URL http://arxiv.org/abs/1402.5945. Extended Abstract in *Proceedings of the 2014 International Symposium on Symbolic and Algebraic Computation ISSAC '14, Kobe, Japan* (2014), 421–428.

MICHAEL ZIEVE (2011). Personal communication. (Cited on page 98.)

MICHAEL E. ZIEVE & PETER MÜLLER (2008). On Ritt's Polynomial Decomposition Theorems. *Submitted,* 38 pages. URL `http://arxiv.org/abs/0807.3578`. (Cited on pages 4, 57, 61, 75, and 79.)

RICHARD ZIPPEL (1991). Rational Function Decomposition. In *Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation ISSAC '91, Bonn, Germany*, edited by STEPHEN M. WATT, 1–6. ACM Press, Bonn, Germany. ISBN 0-89791-437-6. (Cited on page 55.)

K. ZSIGMONDY (1894). Über die Anzahl derjenigen ganzzahligen Functionen n-ten Grades von x, welche in Bezug auf einen gegebenen Primzahlmodul eine vorgeschriebene Anzahl von Wurzeln besitzen. *Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Abteilung II* **103**, 135–144. (Cited on page 9.)

COLOPHON

This thesis was composed on GNU/Linux using Don Knuth's TEX, Leslie Lamport's LATEX, and Hàn Thế Thành's pdfTEX. The references were managed with Oren Patashnik's BIBTEX, the pictures drawn with Till Tantau's Ti*k*Z, and the plots and tables generated with `Sage`.

The font families are Hermann Zapf's *Palatino* and *Euler* for text and mathematics, respectively. The `typewriter text` is set in *Bera Mono* developed by Bitstream, Inc. as *Bitstream Vera*. The typographical look-and-feel is inspired by Robert Bringhurst's *The Elements of Typographic Style* and applied through André Miede's `classicthesis`-package.